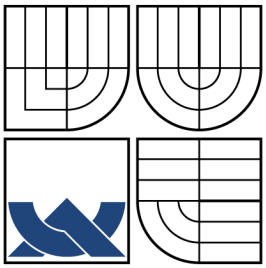
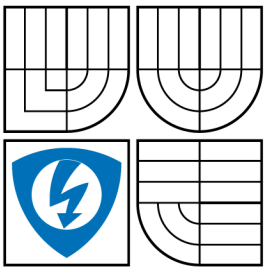


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

DÁLKOVÝ SBĚR DAT PO SILOVÝCH VEDENÍCH

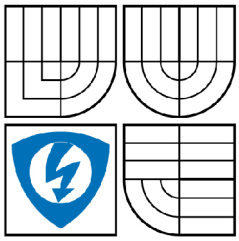
REMOTE DATA ACQUISITION OVER THE POWER LINES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. MARTIN NEUSCHL

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Petr Mlýnek

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Martin Neuschl	***ID:***	80519
Ročník:	2	***Akademický rok:***	2008/2009

NÁZEV TÉMATU:

Dálkový sběr dat po silových vedeních

POKYNY PRO VYPRACOVÁNÍ:

Navrhněte bezpečný způsob autentizace koncových stran v systémech dálkového sběru dat. Sestavte laboratorní pracoviště s PLC modemy. Reálně testujte datovou komunikaci po silových vedeních. Proveďte dlouhodobé testy měření rušení. Zhodnoťte využití silových vedení pro dálkový sběr dat.

DOPORUČENÁ LITERATURA:

[1] Hrasnica, Haidine, Lehnert: Broadband Powerline Communications Network design, ISBN:0-470-85741-2, 2004

[2] Burda.K.: Bezpečnost informačních systémů. FEKT VUT v Brně, 2005.

[3] ModemTec, technická dokumentace modemů PLC. http://www.modemtec.cz.

Termín zadání:	9.2.2009	***Termín odevzdání:***	26.5.2009

Vedoucí práce: Ing. Petr Mlýnek

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ANOTACE

V této diplomové práci na téma „Dálkový sběr dat po silových vedeních“ jsou v prvé řadě rozebrány vlastnosti silových vedení a jejich charakteristika. Dále se dostaneme k přiblížení technologie PLC, její vlastnosti, a využití. Zjistíme, kde vzniká rušení a šum v energetických sítích a v důsledku toho vybereme nejvhodnější modulaci a protichybové kódovaní pro použití v souvislosti s PLC.

V další části si probereme možnosti autentizace, navrhneme bezpečný způsob autentizace pro dálkový sběr dat po silových vedeních a zaměříme se na obranu proti útokům.

Praktická část se zabývá simulací a měřením rušení při komunikaci úzkopásmových PLC modemů firmy Modemtec. Dále se zabývá dlouhodobým testováním energetické sítě a její vliv na rychlost přenosu mezi PLC modemy. Rozebrán je i vliv PLC modemů na primární parametry energetické sítě. Prozkoumány jsou i pakety posílané při komunikaci.

Klíčová slova: autentizace, zabezpečení, dálkový sběr, PLC, elektrická energie,

ABSTRACT

The subject of this paper is „remote data acquisition over the power lines“. The first part is engaged in characteristics of power lines. The other part considers PLC technology, its properties and usage. Base on disturbance and noise in power grid is chosen optimal modulation technique and error handling for PLC.

The next part describes options of authentication. It has been designed secure way of authentication for data collection over power lines and attack-resistance is considered as well.

Practical purpose is dedicated to simulations and noise measuring during communication of narrowband PLC modems. It deals with long-term power grid testing and its influence on transmission rate between PLC modems and also with the influence on primary parameters of power grid. Packets are investigated during communication as well.

Keywords: authentication, security, remote acquisition, PLC, electric energy

Bibliografická citace

NEUSCHL, M. *Dálkový sběr dat po silových vedeních.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 50 s. Vedoucí diplomové práce Ing. Petr Mlýnek.

Prohlášení

Prohlašuji, že svoji diplomovou práci na téma Dálkový sběr dat po silových vedeních jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.
Jako autor uvedeného semestrálního projektu dále prohlašuji, že v souvislosti s vytvořením tohoto projektu jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....
podpis autora

Poděkování

Děkuji vedoucímu diplomové práce Ing. Petru Mlýnkovi z Ústavu telekomunikací za velmi užitečnou metodickou pomoc a cenné rady při zpracování práce.

V Brně dne ……..... ……..

podpis autora

OBSAH

1 ÚVOD

Elektrická energie je přenášena po vedení vysokého napětí a je transformována na nižší napětí, které je použitelné uvnitř budov. Ve všech těchto částech se dá použít komunikace po silových vedeních (PLC).

Komunikace po silových vedeních pracuje na principu modulovaného signálu, který je přiváděn na rozvodový systém.. Vzhledem k tomu, že silové vodiče byly primárně určeny pro přenos střídavého proudu, mají velice omezené schopnosti pro přenos na vyšších frekvencích. Šíření signálu je hlavní problém této technologie.

V této práci si rozebereme vlastnosti silových vedení, jejich vliv na kvalitu přenosu a rušivé vlivy, které se na těchto vedeních vyskytují. Ukážeme si vhodné modulační metody a protichybové kódování pro použití v PLC sítích.

Autentizace koncových stran v sítích dálkového sběru dat je rozebrána v další kapitole, jsou zde možné způsoby autentizace a jejich vhodnost pro použití v těchto sítích. Je také potřeba vytvořit autentizační schéma, které by zabezpečilo danou komunikaci a zabránilo útokům na tyto sítě.

Vlivy na kvalitu přenosu si ukážeme v praxi a zaměříme se na úzkopásmové modemy firmy Modemtec. Zobrazíme si jejich vlastnosti a možnosti rušení jejich komunikace. Dále změříme přenosovou rychlost a ukážeme si vliv modemů na energetickou síť. Prozkoumáme také pakety přenášené modemy po sériové lince.

2 VLASTNOSTI PLC

Přenosový systém v telekomunikačních sítích převádí informační datový tok na použitelnou formu, která je vložena do komunikačního kanálu (nebo média). Jako na všech ostatních komunikačních mediích tak i silová vedení představují útlum a fázový posun signálu. Silová vedení jsou obvykle navrhována jen pro přenos energie a pro připojení daných zařízení a přístrojů. Právě tyto systémy na přenosových cestách způsobují nedostatky pro použití komunikačních signálů. Pro komunikaci po silových vedeních se jeví jako nejlepší pásmo od 100kHz do 30 MHz. Proto pro spolehlivou komunikaci je nezbytné znát vlastnosti vedení v tomto pásmu.

2.1 Charakteristika přenosové cesty

Silové kabely poskytují velice nestabilní kanály kvůli rozdílnosti impedancí, způsobenou různorodostí přístrojů, které jsou připojeny do sítě. Tyto přístroje jsou také konstruovány pro distribuci energie a ne pro přenos dat, kde jsou velice nepříznivé vlastnosti se značným šumem a vysokým útlumem. Z důvodu časové nestálosti parametrů kanálu nelze na nízko napěťové napájecí síti hovořit o ideální charakteristické impedanci a z toho plyne problematika vícecestných úniků, což je způsobováno odrazy vznikajícími impedančním nepřizpůsobením v kabelových větvích. Impedance silových kabelů se opět značně mění s frekvencí a v závislosti na umístění. Impedance se mění v rozsahu od několika ohmů do několika kiloohmů. Impedance je hlavně ovlivněna charakteristickou impedancí kabelu, topologií zvažované sítě a množstvím připojených zařízení. Střední hodnota impedance roste spolu s frekvencí, z čehož se dá usoudit, že vedení má induktivní charakter. Statistické analýzy ukazují, že téměř celé spektrum je střední hodnota impedance mezi 100 až 150Ω. Nicméně pro frekvence menší než 2MHz má tato střední hodnota tendenci se snižovat a dosahuje hodnot od 30 do 100Ω. Hodnoty útlumu mohou být až 60dB. Měnící se impedance, nevhodné připojení přístrojů a výsledné přenosové ztráty, jsou hlavní problém PLC sítí.

2.1.1 Model sítě

Model parametrů kanálu je obvykle založen na studiu přenosové funkce a přídavného šumu. Parametry kanálu se příliš s časem nemění v porovnání s typickou symbolovou periodou. Přenos mezi dvěma body je zejména ovlivněn třemi parametry.

Délkou , typem kabelů a rozsáhlostí větvení. K realizaci modelu je možné využít spoustu přístupů. Většina je založena na chování prvků v síti a jejich rozložení. Tento přístup vede k velkému množství parametrů, z nichž některé je těžké vyčíslit. Odlišný a jednodušší přístup je nahlížet na kanál jako na krabičku, která je popsaná přenosovou funkcí mezi vstupem a výstupem.

2.2 Vlastnosti síťových kabelů

Podle [5] elektrické vlastnosti vedení z hlediska přenosu určují **primární parametry** vedení: odpor R[Ω/km], indukčnost L[H/km], kapacita C [F/km] a svod [S/km]. Tyto parametry nejsou závislé na napětí a procházejícím proudu, ale závisí na konstrukci vedení, jeho materiálu a přenosové frekvenci. Uvažujeme-li dvouvodičové homogenní vedení, můžeme jeho impedanci, nazývanou jako **charakteristická impedance**, při určité frekvenci ω popsat rovnicí:

$$Z_C = \sqrt{\frac{R + jwL}{G + jwC}} \tag{2.1}$$

$$g = \sqrt{(R + jwL)(G + jwC)} \tag{2.2}$$

Představuje komplexní veličinou a lze ji vyjádřit tvarem

$$g = a + jb \tag{2.3}$$

Parametr α je označován jako **měrný útlum** a jeho jednotka je dB/km a mění se s vlastnostmi vedení. Pokud tuto hodnotu vynásobíme délkou vedení v kilometrech dostaneme **útlum** v decibelech.

Parametr β je nazýván jako měrný **fázový posuv** [rad/km], pokud se opět vynásobí délkou vedení v kilometrech dostaneme **fázový posuv** [rad].

Pro vysokofrekvenční použití v PLC (1-30MHz) můžeme rovnice (2.1) a (2.2) zjednodušit za podmínek, že R << ωL a G << ωC a potom dostáváme:

$$Z_C \cong \sqrt{\frac{L}{C}} \tag{2.4}$$

2.3 Kmitočty pro přenos

2.3.1 Pásmo 3-148,5kHz

Podle [7] je pásmo 3-148,5kHz v Evropě pro přenos dat po elektrické síti stanoveno evropskou normou EN 50065-1 [14]. Norma rozděluje toto pásmo do 4 dílčích pásem. Ale z hlediska dosavadních pozorování o zdrojích rušení, jako jsou tyristorové regulátory, sériové motory a komunikační kanály rozvodných závodů (v České republice velice rozšířený systém HDO), se jako spodní hranice pro komunikaci po silových vedeních uvažuje 100kHz. Horní hranice je dána normou a souvisí s rušením vysilači pracujících na dlouhých vlnách (AM), je to přibližně 150kHz.

Pásmo	Rozsah	Užití
	3-9kHz	omezeno pro dodavatele el. Energie
A	9-95kHz	pro dodavatele a pro spotřebitele se souhlasem dodavatele
B	95-125kHz	jen pro odběratele
C	125-140kHz	jen pro odběratele spolu s přistoupením k dohodě
D	140-148,5kHz	jen pro odběratele

Pro všeobecné použití je možné použít pásma B, C, D. Z tabulky je možné vyčíst, že daná pásma nejsou nějak široká a z toho plyne omezená a nízká přenosová rychlost.

Protokol o přistoupení k dohodě normy EN 50065-1 převzatý od [7]:

- všechny systémy musí použít kmitočet 132,5kHz k upozornění, že vysílání pokračuje
- žádný vysílač nesmí vysílat spojitě po dobu přesahující 1s a po každém vysílání nesmí vysílat znovu po dobu alespoň 125ms (Vysílání je považováno za řadu signálů, v kterých není mezera větší než 80ms)
- každý vysílač musí být vybaven signálním detektorem, který detekuje, kdy je pásmo v použití. (tj. stav, kdy jakýkoliv signál o efektivní hodnotě 80dB v pásmu 131,5-133,5kHz trvající alespoň 4ms, je přítomen na hlavních vstupních svorkách přístroje)
- přístroj může vysílat, jestliže pásmo není využito po dobu v každém případě náhodně zvolenou a rovnoměrně rozloženou mezi 85ms a 115ms alespoň sedmi možnými hodnotami v tomto pásmu

- k umožnění detekce použitého pásma musí přístroj vysílat svůj signál se spektrálním rozložením v souladu s B přílohou této normy

Výstupní napětí vysílače v pásmu od 3 do 9kHz je 89dB (1V). V pásmu od 9 do 148,5kHz kvazišpičková hodnota klesá lineárně s logaritmem kmitočtu z hodnoty 89dB na hodnotu 66dB.

2.3.2 Pásmo 2-30MHz

Pro velké objemy dat je nutné použít vysokofrekvenční pásma. Komerční systémy PLC používají pro přenos frekvence od 2 do 30MHz. To umožňuje daným systému použít fyzické přenosové rychlosti až 200Mbit/s. Pásma jsou dynamicky řízena tak, aby docházelo k co nejlepší propustnosti dat po silových vedeních. Toto pásmo je opět rozděleno do několika dílčích pásem na základě rozsáhlých měření a zkoušek a plánováním v rámci krátkovlnného pásma, které je vedeno Evropským výborem pro elektrotechnickou standardizaci (CENELEC). V současnosti se překládá v členských státech Evropské unie návrh evropské normy (prEN59013).

Používají se až tři pásma od 2 do 13MHz pro venkovní použití a až tři pásma od 15 do 30MHz pro vnitřní použití. Nízké frekvence byli vyhrazeny pro venkovní použití díky nízkému útlumu. Pásma lze z hlediska místního zarušení rádiovými frekvenčními signály přepínat z jednoho na druhé a lze tyto pásma deaktivovat. Tyto pásma zajišťují uživatelům rychlosti od 700 do 1500kbit/s a jsou závislé na kvalitě připojení.

2.4 Využití PLC

2.4.1 Domácí počítačová síť (LAN)

Komunikace po silových vedeních může být také použita pro menší domácí počítačovou síť. Do sítě je možné pomocí adaptérů připojit v podstatě všechny prvky se síťovou technologií LAN. Prozatím však ještě nebyl schválen jednotný standard a proto každá firma používá odlišný způsob technologie.

2.4.2 Poskytování internetového připojení

Technologii PLC lze použít i pro poskytování internetového připojení. Počítač je však nutno připojit přes “PLC modem“ do elektrické sítě. Výhodou je rozsáhlá infrastruktura elektrických sítí a v odlehlých místech s elektrickou přípojkou nízké

náklady na zřízení přípojky. V současné době se však nejedná o standardní připojení. Poskytování internetového připojení po elektrických sítích má za sebou více pádů než úspěchů. Jedinou zemí, kde se tato technologie rozrostla, je Německo.

2.4.3 Domácí automatizace

Elektrické vedení se v domácnosti může používat jako přenosové medium pro jiné technologie. Tyto přenosy se používají pro ovládání osvětlení, různých přístrojů a měřících zařízení v oblasti domácí automatizace. Systém pracuje ve spolupráci s řídícím počítačem, který je možno ovládat i dálkově. Řízení celého domu z jednoho místa je samozřejmostí. Výhoda je, že se nemusí složitě instalovat další kabely pro ovládaní, stačí pouze elektrické rozvody.

2.4.4 Dálkový sběr dat

V soustavách pro distribuci energií je pro distribuční společnosti důležitou věcí znát údaje o výstupech, tj. o odběrech uživatelů, vlastních nákladech, ztrátách či jiná data. Vzhledem k tomu, že jde o velice rozsáhlé soustavy, jsou tyto údaje shromažďovány pochůzkou pracovníků společnosti. Je to velice náročné na čas a finanční prostředky, proto společnosti hledají řešení jak tento sběr zjednodušit a zefektivnit. Jedním ze způsobů je dálkový sběr dat, kdy se po silových vedeních shromažďují údaje od jednotlivých uživatelů a zařízení v síti. Jedná se o velice efektivní a automatizovaný sběr dat.

Jak už název práce napovídá, budeme se zaobírat zejména touto technologií.

2.4.5 Nízkofrekvenční komunikace

Nízké frekvence používají zejména rozvodné závody pro ovládání a regulaci spotřeby elektrické energie a telemetrii. Frekvence v řádu sta Hz se používají pro systém hromadného dálkového ovládání (HDO). Systém ovládá elektrické spotřebiče na dálku, tarifní programy a další včetně synchronizace hodin.

3 RUŠENÍ A ŠUM

3.1 Vlastnosti šumu

Protože jsou silové kabely konstruovány pouze pro přenos energie, nikde nenajdeme vlastnosti těchto medií ve vysokofrekvenčním rozsahu. Kromě toho je do silových sítí připojeno velké množství zařízení z různými vlastnostmi. Proto se před použitím těchto medií pro přenos informací provede intenzivní šetření jevů přítomných v tomto prostředí. Kanály na silových vedeních obsahují rušení hodně vzdálené od typického aditivního bílého šumu (AWGN), přítomného v telekomunikačních kanálech, který má po celé přenosové spektrum konstantní výkon.

Bylo provedeno mnoho měření a šetření, aby byly podány co nejlepší detailní výsledky o vlastnostech rušení v PLC zařízeních. Zajímavý popis je uveden v článku [3], který dělí šum jako superpozici pěti typů šumu, dělených podle jejich zdroje, době trvání, obsazení spektra a intenzity.

Barevný šum pozadí [1], jeho výkonová spektrální hustota je poměrně nízká a klesá s frekvencí. Tento typ šumu **je hlavně způsobován skládáním četných zdrojů šumu nízké intenzity**. Na rozdíl od bílého šumu, který je náhodný, spojitý a má stálou spektrální hustotu nezávislou na frekvenci a na předepsaném frekvenčním rozsahu, barevný šum pozadí ukazuje silnou závislost na uvažovaných frekvencích. Parametry tohoto šumu se mění s časem v čase minut a hodin.

Úzkopásmový šum [1], který má po většinu času sinusovou podobu s modulovanými amplitudami. Tento typ obsazuje většinu dílčích pásem, které jsou relativně malé a souvislé po celém frekvenčním spektru. Tento šum **je způsobován pronikáním vysílání na středních a krátkých vlnách od pozemních rádiových vysílačů**. Jeho amplituda se obecně mění s denním cyklem, kdy se při příchodu noci zvětšuje, protože odrazové vlastnosti atmosféry se zlepšují.

Periodický impulsní šum, nezávislý na síťové frekvenci [1], má tvar impulzů, které se většinou opakují v intervalu od 50 do 200kHz a ve výsledném spektru se zobrazují jako diskrétní linky s frekvencemi odpovídající opakovacímu kmitočtu. Tento typ šumu **je způsobován spínáním zdrojů energie**. Protože má tento šum vysokou opakovací

frekvenci, obsazené frekvence jsou vzájemně velice blízké a sestavují proto frekvenční svazky podobné úzkým pásmům.

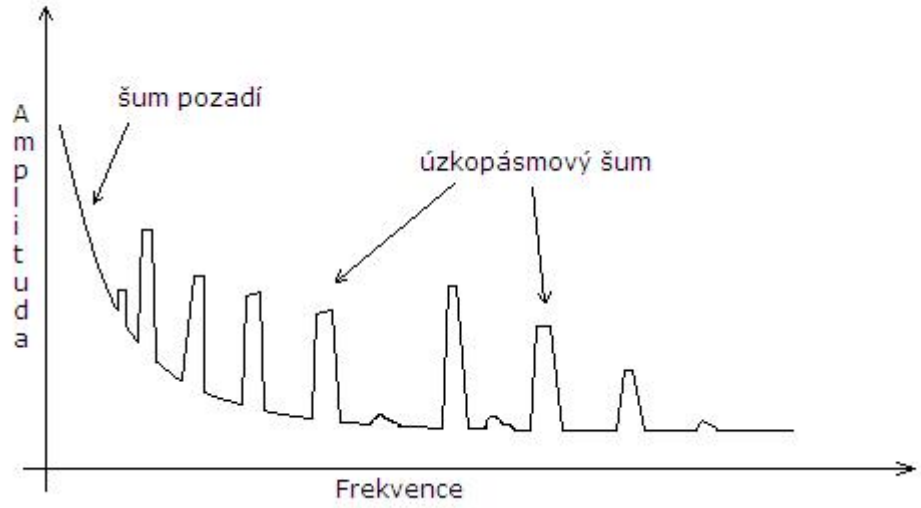
Periodický impulsní šum, synchronní se síťovým kmitočtem [1], je impulsní s opakovací frekvencí 50 nebo 100 Hz a je synchronní se síťovým kmitočtem na silovém vedení. Tyto impulzy mají krátkou dobu trvání, řádově mikrosekundy, a výkonová spektrální hustota klesá s frekvencí. **Je způsobován spotřebiči s usměrňovači a univerzálními sériovými motory**.

Asynchronní impulsní šum [1], jeho impulsy **jsou způsobeny spínáním v síti**. Tyto impulsy mají dobu trvání v řádu od mikrosekund až do milisekund s chaotickým intervalem. Jejich výkonová spektrální hustota může dosáhnout hodnot větších než 50dB nad úroveň šumu v pozadí a řadí tento typ šumu mezi hlavní příčiny chyb v komunikaci přes PLC sítě.

Barevný šum pozadí, úzkopásmový šum a periodický impulsní šum, nezávislý na síťové frekvenci zůstávají obvykle neměnné po delší časové úseky v řádech sekund, minut a někdy i hodin. Proto se tyto tři typy šumu zahrnují do jednoho, který je uváděn jako **celkový šum pozadí**. Periodický impulsní šum, synchronní se síťovým kmitočtem a asynchronní impulsní šum se naopak mění v čase v řádu milisekund a mikrosekund a můžeme je popsat jako **impulsní šum**. Protože má tento typ šumu relativně vysoké amplitudy, způsobuje shluk chyb vznikající v přenosu signálu na vysokých frekvencích přes PLC.

3.2 Celkový šum pozadí

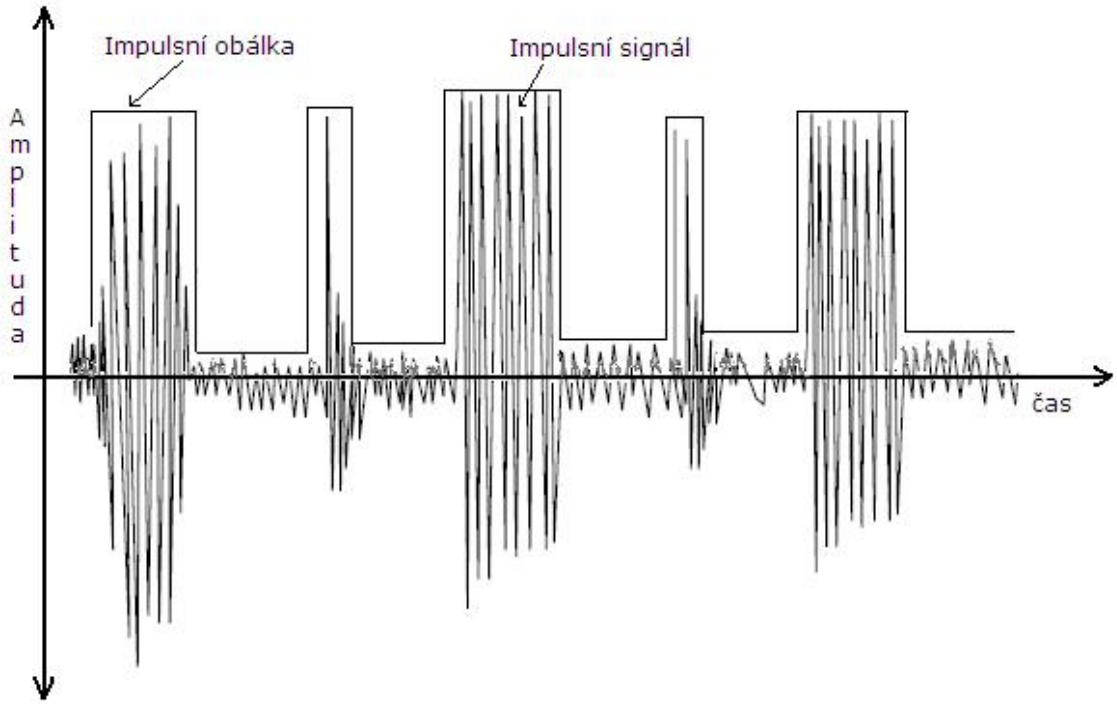
Pro představu je tento celkový šum pozadí v PLC sítích superpozicí barevného šumu pozadí a úzkopásmového rušení (obr. 1). V tomto případě se nedělají rozdíly mezi krátkovlnným rádiovým a jiným úzkopásmovým rušením ve spektru, protože normálně jsou spektrální čáry neomezené. Pro naši představu jsou aproximovány na jejich obálky. Kvůli vysoké opakovací frekvenci šumu typu 3 obsazuje tento šum vzájemně velice blízké frekvence a vznikají proto frekvenční svazky. Proto se modeluje jako úzkopásmový šum s velice nízkou spektrální výkonovou hustotou.



Obr. 1: Celkový šum pozadí

3.3 Impulsní šum

Impulsní šum je považován za nejnebezpečnější [1]. Má charakter krátkých vysokofrekvenčních impulsů o vysoké amplitudě, které se střídají s delšími klidnými intervaly. Dosavadní pokusy dokázaly, že v tomto druhu šumu výrazně dominuje asynchronní impulsní šum. Proto pro další studium budeme uvažovat pouze tento šum, zobrazený na obrázku (Obr.2).



Obr. 2: Příklad impulsního šumu

Podle článku [3] měřené impulsy mají z 90% amplitudu mezi 100 a 200mV. Jenom méně než 1% má amplitudu větší než 2V. Měření také dokázaly, že délka jednotlivých impulzů překračuje pouze v 1% délku 500μs a v 0,5% délku 1ms. A nakonec čas oddělující jednotlivé impulsy je pod 200ms ve více než 90% případech.

4 MODULAČNÍ METODY V PLC

Výběr modulační metody pro daný komunikační systém silně souvisí s prostředím a s vlastnostmi média, na kterém bude probíhat komunikace. Silové kabely poskytují nevhodné vlastnosti pro přenos komunikačních signálů, jako šum a vícecestnost kanálů. Kromě nízkých nákladů, musí modulace pro PLC překonat i tyto kanálové chyby. Například modulace pro realizaci PLC systému musí být schopna zdolat nelineární charakteristiku kanálu. Tato nelinearita dělá demodulátor, pokud je to možné, pro rychlosti okolo 10Mbps s jednou nosnou frekvencí, velice složitý a nákladný. Proto musí modulace překonat tyto problémy bez potřeby složitého opravování. Impedanční nesouvislosti v silových vedeních přecházejí v odrazy způsobující šíření zpoždění, a tyto problémy musí opět překonat modulace. Zvolená modulace musí nabízet vysokou flexibilitu v použití a/nebo vyloučení některých frekvencí, pokud jsou tyto frekvence velice zarušeny a nebo jsou lokálně zakázány pro použití v PLC signálech.

Pro PLC systémy přichází vhod hned několik modulačních metod [2]. Nejjednodušší a nejvýhodnější jsou metody založené na úzkopásmové modulaci o jedné nosné. Jsou to například **frekvenční klíčování** (FSK), **fázové klíčování** (PSK) a podobné. Tyto metody lze použít pouze pro nízké bitové rychlosti, protože širokopásmové využití je z důvodu vysoké mezisymbolové interference (**ISI – Inter Symbol Interference**) značně omezeno. Při vyšších přenosových rychlostech by docházelo ke zbytečné složitosti demodulátoru. Tyto modulace se používají v pásmu okolo 100kHz a pro přenosové rychlosti v řádu desítek kb/s. Proto se pro zvýšení přenosové rychlosti používá širokopásmových přenosů od 2 do 30 MHz. V tomto pásmu se nabízí k použití **kódové dělení** (CDMA) ve variantě DSSS, které je vhodné pro rychlosti v řádech jednotek Mbps. Tato technika poskytuje imunitu proti rušení úzkopásmovým šumem, ale výhoda sdílení přenosového pásma několika uživateli se zdá být málo využitelná. Signál od jednoho uživatele může být zcela zamaskován bližším uživatelem, jehož signál může být o desítky decibelů silnější. Pomocí DSSS je poměrně složité levně a efektivně realizovat synchronizaci, tento problém však odpadá na silových rozvodech, kde je k dispozici stabilní síťový kmitočet.

Současné studie se zaměřují na dvě nejvhodnější modulační techniky, které předvádí dobré výkony v jiných složitých zařízeních a proto jsou vhodné pro aplikaci v odlišných systémech s širokým zaměřením. První modulace je **ortogonální multiplex s kmitočtovým dělením** (OFDM), která je použita v technologiích DSL a dalších a řeší

problematiku ISI. Druhá modulace, **rozprostřené spektrum**, se široce používá v bezdrátových aplikacích, nabízí přijatelnou modulaci aplikovatelnou na velký rozsah mnohonásobného přístupu.

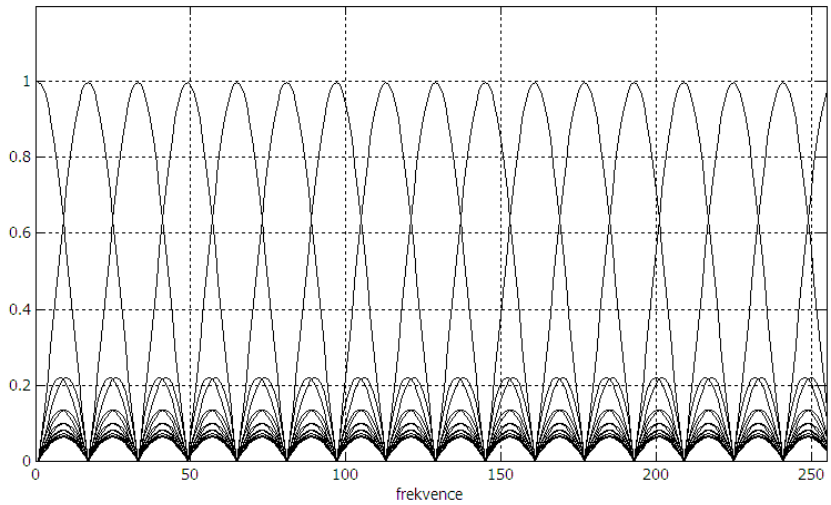
V této části se budeme zabývat těmito modulačními technikami a jejich možnostmi pro použití v PLC. Nakonec provedeme porovnání těchto modulací a diskuzi jejich výhod a nevýhod.

4.1 OFDM (ortogonální multiplex s kmitočtovým dělením)

Modulace OFDM [6] se s úspěchem používá při pozemním vysílání digitální televize DVB-T (Digital Video Broadcasting) nebo digitálního rozhlasu DAB (Digital Audio Broadcasting). Variace OFDM se v poslední době využívá i v technologii ADSL, kde představuje modulaci OFDM s adaptivním bitovým vytěžováním, takzvané DMT (Discrete MultiTone). V neposlední řadě se používá u bezdrátových sítí standardu 802.11a nebo 802.11g.

Princip činnosti modulace je v rozdělení přiděleného pásma na větší počet samostatných frekvenčních kanálů a každý z nich přenáší samostatný signál. Nosné jsou podle potřeby modulovány dle potřeby různými modulacemi (QPSK, 16QAM, 64QAM). Jednotlivé nosné jsou vzájemně ortogonální, to znamená, že maximum nosné se překrývá s minimem ostatních nosných. Celkový datový tok kanálu se dělí na dílčí datové toky jednotlivých kanálů.

Při přenosu se v reálném čase vyhodnocuje chybovost jednotlivých dílčích kanálů, jak moc se projevuje rušení, zkreslení a jiné vlivy. Podle míry chybovosti jednotlivého kanálu se pak použije pro přenos signálu, nebo naopak ne. Samotná modulace probíhá s nízkou modulační rychlostí, aby se co nejméně projevoval odraz signálů. Přenosová kapacita silových vedeních se může dynamicky měnit na základě toho, jaký je momentální stav sítě a rušení v ní.



Obr. 3: Frekvenční spektrum OFDM

4.2 Rozprostřené spektrum

Rozprostřené spektrum [6] je typ modulace, která rozprostře data tak, aby mohla být přenesena celým dostupným frekvenčním pásmem. Děje se tak v širším pásmu, než je ve skutečnosti pro přenos potřebné. První systém rozprostření spektra byl navržen pro bezdrátové digitální komunikace tak, aby překonal útoky, kdy někdo zamýšlí přerušit komunikaci. Tuto modulaci je velice nesnadné detekovat, o takto modulovaném signálu se říká, že je podobný šumu, a stejně těžké je signál rušit. Systém byl navržen pro vojenské použití, avšak si našel velké uplatnění v civilní sféře. Jeho aplikace je typická pro bezdrátové telefony, bezdrátové sítě LAN, Bluetooth a systémy PLC. Většinou neexistuje žádná kontrola ohledně vysílání a systém pracuje v přítomnosti silných interferencí s jinými komunikačními systémy. V tomto případě není rušení úmyslné, ale elektromagnetické interference mohou způsobovat rušení systémů, které nejsou modulované rozprostřeným spektrem, ale pracují ve stejném pásmu.

Běžné techniky rozprostření spektra jsou DS (Direct Sequence), FH (Frequency Hoping), TH (Time Hopping) a MC (Multi Carrier). Samozřejmě jde tyto techniky různě kombinovat a vytvořit hybridní systém, který má výhody rozdílných technik. Pro PLC se hodí pouze DS a FH. Rozvedeme si pouze systém DSSS (Direct Sequence Spread Spectrum).

4.2.1 DSSS

DSSS (Direct Sequence Spread Spectrum) [6] je technika přímého rozprostření spektra. Je jednou z nejpoužívanějších metod pro rozšíření spektra při bezdrátovém přenosu. Pracuje tak, že každý bit určený k přenosu, je nahrazen sekvencí několika bitů (tzv. chipů). Tyto sekvence mají většinou pseudonáhodný charakter. Na nosný signál je pak modulována pouze tato sekvence bitů. Uměle se tak zavádí nadbytečnost (redundance), která se při datových přenosech používá pro větší spolehlivost přenosů. Zde je ale důvod jiný. Signál je díky této redundanci rozprostřen do větší části spektra a díky tomu je méně citlivý na rušení. Ostatní uživatelé vidí signál jako náhodný šum a bez znalosti mechanismu vytváření je velice obtížné nemodulovat přenášená data. Tato modulační technika se používá v bezdrátové síti Wifi nebo v navigačním systému GPS.

4.3 Vhodná modulace pro PLC

Největší nevýhodou techniky rozprostřeného spektra oproti modulaci OFDM je nízká realizovatelná rychlost přenosu. Právě tento rozdíl v obou modulacích dělá rozhodnutí pro použití modulace v PLC velice těžké. Hlavní výhodou techniky rozprostřeného spektra je elektromagnetická kompatibilita u záření slabých elektromagnetických polí v prostředí. Pro správnou volbu modulace je vhodné znát, jaké jsou nároky a priority navrhované sítě. Vysoká realizovatelná rychlost přenosu u OFDM ukazuje vysokou odolnost proti kanálovým poruchám a flexibilitu ve výběru přenosových kanálů spolu s optimálním využitím přiděleného pásma.

Kvůli své schopnosti poradit si s rušení je modulace OFDM nejvhodnějším kandidátem pro širokopásmové komunikace po silových vedeních. Řeší problematiku ISI, efektivněji využívá přidělená pásma a použití OFDM též zjednodušuje kanálovou ekvalizaci.

5 PROTICHYBOVÉ KÓDOVÁNÍ

5.1 Vznik chyb

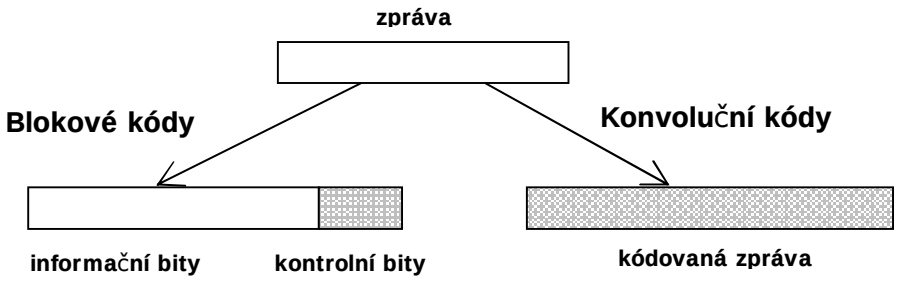
PLC sítě musí pracovat se signálem, jehož výkon musí být pod limitem definovaným *regulačními úřady*. Na druhou stranu musí mít signál takový výkon, aby byl možný datový přenos. To znamená, že by měl být dostatečný odstup výkonu signálu od výkonu šumu. Dokud nebude tento odstup dostatečný, protichybové kódování nebude mít žádný účinek. Nejvíce chyb v PLC sítích způsobuje impulsní šum, který má mnohem větší výkon než šum pozadí. V tomto případě už není odstup dostatečný, aby překonal poruchy a dochází ke vzniku chyb. Pokud je délka trvání těchto impulsů relativně krátká, fyzická vrstva se s těmito chybami sama vypořádá. Naopak pokud jsou impulsy delší, jsou potřeba přídavné mechanismy pro protichybové kódování a opakovaný přenos.

5.2 Princip

Principem u bezpečnostních kódů podle [6] je, že vysílací kodér podle daných pravidel vloží do zprávy mimo **informačních bitů** i tzv. **kontrolní bity**. Úkolem dekodéru na přijímací straně je ověřit jestli přijaté kontrolní bity ve zprávě vyhovují stanoveným pravidlům. Pokud ano, kodér odstraní tyto kontrolní bity a informační bity předá nadřízené vrstvě. Pokud nevyhovují, existují dvě možnosti. V první možnosti je použitý tzv. **detekční kód**, který dokáže chyby pouze odhalit. V tomto případě si dekodér vyžádá u vysílače opětovné odeslání zprávy. Toto se opakuje do té doby, něž dekodér nedetekuje žádnou chybu nebo nepřekročí maximální počet opakování. Tento postup se popisuje jako protokol **ARQ** (Automatic Repeat Request). Ve druhé možnosti je použit tzv**. korekční kód**, který výskyt chyb umí nejen detekovat, ale umožňuje chybu i nalézt a sám ji opravit. V případě chyby tuto chybu opraví a předá zprávu nadřízené vrstvě. Protokol se označuje zkratkou **FEC** (Forward Error Correction). Protokol ARQ se používá pokud je k přenosu použit kanál s nízkou chybovostí, kde je nízká pravděpodobnost výskytu chyb a tím daná malá potřeba opakování. U protokolu FEC je zapotřebí k informačním bitům přidat více kontrolních bitů než u protokolu ARQ. Proto se protokol FEC používá v kanálech s vysokou chybovostí. Tento protokol je upřednostněn pro použití v oblasti přenosu dat po silových vedeních, kde je velká pravděpodobnost výskytu chyb.

5.3 FEC (Forward Error Correction)

FEC [6] je široce používaná metoda používaná pro zlepšení spojení v digitálních komunikacích. Jak název napovídá jeho výhoda je v tom, že korekce chyb vzniklých při přenosu probíhá v přijímači bez nutnosti opakování přenosu. Hlavní funkce FEC je v přidání určitého množství redundantní informace, která pomůže přijímači opravit chyby vzniklé při přenosu vlivem zkreslení a šumu. Podle teorie přenosu informace má každý přenosový kanál teoretickou maximální kapacitu, která záleží na šířce pásma a odstupu signál-šum (SNR). Kapacita realizovaných systémů je obvykle mnohem nižší než maximum podle této teorie. Proto se používají vhodné kódy, které dovolují zlepšení efektivity využitelnosti přenosového pásma.



Obr. 4: Rozdělení FEC

Korekční kódy mohou být rozděleny do dvou hlavních skupin: **blokové kódy** a **konvoluční kódy**, jak je vidět na Obr.3. Blokové kódy na základě informačních bitů produkují kontrolní bity konstantní délky, které přidávají do zprávy. Oproti tomu konvoluční kódy generují upravenou zprávu z nadbytečnými informacemi a kódovaná zpráva je delší.

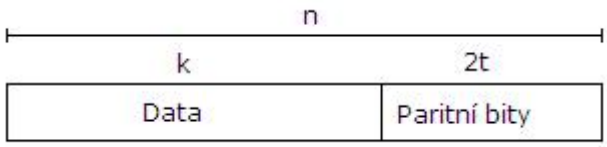
5.4 Blokové kódy

Charakteristické na blokových kódech je to, že je zpráva nejprve rozdělena na bloky o konstantní délce k bitů (tzv. zdrojové slovo) a tyto bloky jsou poté transformovány na zabezpečené bloky, každý o délce n bitů a platí n > k. Takovýto kód se symbolicky označuje jako kód (n, k).

Blokové kódy mohou být řazeny do dvou kategorií: binární a nebinární kódy. Příkladem binárních blokových kódů mohou být: cyklický, hamming, BCH. Nebinární kódy pracují na principu symbolů sestávajících z více než jednoho bitu. Nejpopulárnější v telekomunikační technice jsou Reed-Solomonovy (RS) kódy, které jsou odvozené z binárního BCH kódu. RS kódy mají vysokou schopnost opravovat shluky chyb.

5.4.1 Reed-Solomonovy kódy

Tyto kódy se označují zkratkou RS (n,k), která daný kód charakterizuje. RS kódy jsou kódy blokové, proto platí stejná charakteristika jako v předchozím odstavci. Reed-Solomonův dekodér je schopen opravit maximálně t chybných symbolů a zároveň platí, že 2t = n – k. RS kód tedy na vysílací straně přidá k blokům dat redundantní bity a pomocí těchto bitů dekodér opraví chyby vzniklé při přenosu. Počet opravitelných chyb záleží na parametrech RS kódu. Přenášený blok je znázorněn na následujícím obrázku.



Obr. 5: Přenášený blok

Tento kód je pro své dobré vlastnosti používán v mnoha digitálních zařízeních. Jedná se například o GSM, DVB nebo data na discích CD a DVD. Pokud se vyskytnou při přenosu shlukové chyby, které nedokáže kód zpracovat, použije se tzv. prokládání dat (interleaver), které rovnoměrně rozprostře chyby do větších úseků.

5.5 Konvoluční

U konvolučních kódů je redundance, která musí být přidána kvůli předcházení chyb, spojitě rozdělena do bitového toku. Na rozdíl od blokových kódů, které pracovaly s konečnou délkou jednotlivých bloků, konvoluční kodér pracuje se spojitou sekvencí symbolů.

5.6 Vhodné kódování pro PLC

Vzhledem k vysoké chybovosti přenosového kanálu u silových vedeních se pro přenos nehodí systém ARQ, u kterého by opětovné odesílání zpráv bylo velice neúnosné a z hlediska k omezeným přenosovým rychlostem i neefektivní. Proto musíme použít systém FEC spolu s korekčním kódem. V prostředí vysoké chybovosti se úspěšně používají Reed-Solomonovy kódy ve spojení s modulací OFDM. Tento přenosový systém lze s úspěchem použít i v sítích PLC. Typ RS kódu se určí podle využití sítě a její chybovosti.

6 AUTENTIZACE KONCOVÝCH STRAN

Autentizace je obecně proces, při kterém se ověřuje identita protější strany. Neboli zda je uživatel či entita na druhé straně drátu skutečně tím, za koho se vydává. U dálkových systémů je toto největší problém. Autentizace se provádí pouze jednou při navazování spojení.

6.1 Autentizační prostředky

V této kapitole jsou rozebrány možnosti autentizace [8] a jejich použití pro dálkový odečet dat v PLC sítích.

6.1.1 Autentizace znalostí

Pracuje na principu kontroly určité informace, před samotným povolením přístupu. Tato informace je známa pouze uživatelům a útočník by k ní neměl mít přístup. Informace má podobu řetězce alfanumerických znaků (heslo) nebo řetězce numerických znaků (autentizační kód), a to z důvodu jednoduché zapamatovatelnosti v uživatelově paměti. Autentizace heslem je jedním ze základních autentizačních prostředků.

Hlavním nedostatkem je přenos samotného hesla k systému. Existuje několik způsobů jak heslo přenést. Od přenosu v otevřené podobě až po aplikaci volitelné jednosměrné funkce na heslo. Avšak platí, že útočník je schopen při delším odposlouchávání heslo vždy odhalit. Tato autentizace se dá spolehlivě použít právě tam, kde je dlouhodobý odposlech komunikace nemožný. Toto pravidlo neplatí pro PLC sítě, proto tento způsob komunikace je nedostatečný.

6.1.2 Autentizace žadatelem

U tohoto druhu autentizace se identita ověřuje porovnáním aktuálně zjištěných charakteristik žadatele s uloženým záznamem těchto charakteristik [8]. Tyto charakteristiky se proto musí nejprve u žadatele zjistit a následně důvěryhodným a bezpečným způsobem uložit. Podle míry shody pak systém rozhoduje o povolení přístupu.

Při volbě charakteristik je nutné brát ohled na jejich individualitu a neměnnost, v neposledním případě také na finanční náklady a rychlost pořízení charakteristiky. Tato autentizace se vzhledem k individuálnosti používá pouze u osob. Sledované charakteristiky se vyjadřují v číselné podobě (biometriky) a autentizace na nich

založená se nazývá **biometrická autentizace** [8]. V současné době jsou biometrické metody rozděleny do dvou základních tříd:

- fyziologické metody
  jsou založeny na fyziologických vlastnostech člověka (např. otisk prstu, obličej, DNA)
- behaviorální metody
  jsou založeny na způsobu chování člověka (např. jeho podpis)

Tyto metody autentizace jsou pro systémy dálkového sběru dat nevhodné, a to z důvodu veliké vzdálenosti mezi centrem a jednotlivými sběrnými místy.

6.1.3 Autentizace předmětem

- **Autentizátory**

Jsou to elektronické pomůcky pro autentizaci uživatele [15]. Jsou vybaveny autentizačním kalkulátorem, který sdílí určité sdílené tajemství. Součástí je také algoritmus pro vytváření kontrolních součtů a zdroj přesného času. Kalkulátory jsou schopny generovat jednorázová hesla, tvořena za pomoci času a sdíleného tajemství. Nevýhodou těchto kalkulátorů je závislost na přesnosti zdroje času a jeho synchronizaci. Pro odbourání této závislosti může kalkulátor počítat několik hesel dopředu i dozadu a ty pak porovnávat.

- **USB tokeny**

Jádrem těchto tokenu je inteligentní kryptografický čip, většinou s vlastním operačním systémem, vnitřní pamětí a komunikačním rozhraním USB [15]. Operační systém zajišťuje komunikaci, autentizaci a volání jednotlivých kryptografických operaci:

- generování asymetrického páru klíčů
- import asymetrického páru klíčů
- úložiště osobních certifikátů
- úložiště kořenových certifikátů CA
- elektronický podpis daným privátním klíčem

Generováním privátního klíče přímo na tokenu je odstraněn problém, že nemůže existovat jiná kopie klíče. Navíc tyto tokeny při každém použití vyžadují autentizaci uživatele pomocí PINu. Tímto je privátní klíč chráněn dvoustupňovou autentizací.

- **Čipové karty**

Jádrem těchto karet je čip, který je umístěný v plastové kartičce [15]. V čipu je integrován kryptografický procesor , paměťový modul a vstupně-výstupní prostředky. Mikroprocesor bývá většinou 8-mi bitový. Karty dělíme na kontaktní a bezkontaktní.

6.2 Autentizační protokoly

6.2.1 Základní

Je nejjednodušším způsobem ověřování a probíhá následovně. Klient nejprve odešle serveru požadavek na získání informací. Server odpoví zprávou „přístup odepřen“ a žádá klienta o přihlašovací údaje. Tyto údaje následně klient serveru odešle. Tyto data nejsou při přenosu šifrovány, proto tato metoda není odolná vůči útokům. Tento typ autentizace je vhodné použít s vhodným šifrovacím protokolem.

6.2.2 Výzva-odpověď

Protokoly typu výzva-odpověď jsou založeny na tom, že strana, která žádá o autorizaci, prokáže znalost informace, aniž by tuto informaci prozradila kterémukoliv jinému subjektu. To je dosaženo pomocí časově proměnné výzvy. Tato výzva musí být pro každou autorizaci jedinečná, aby nedošlo ke zneužití komunikace pomocí odposlechu. Strana ověřující identitu odešle protistraně neopakovatelnou výzvu s náhodnou hodnotou. Protistrana provede nad výzvou výpočet, do kterého zahrne i tajnou informaci a výsledek spolu s dalšími volitelnými údaji odešle zpět. Autentizace pak spočívá v kontrole správnosti těchto údajů. Náhodnou hodnotu lze získat několika způsoby, a to jako:

- **Náhodné číslo**. Je to číslo nepředvídatelné. Kromě opravdu náhodných čísel, které lze velmi těžko odhalit, se v praxi používá i čísel pseudonáhodných.
- **Sekvenční číslo**. Sekvence je monotónní rostoucí posloupnost čísel. Výzva je tvořena touto posloupností následující po naposledy použité hodnotě. Proto si obě strany musí pamatovat poslední hodnotu.
- **Časové razítko**. Získává se za použití aktuálního času. Komunikující strany musí mít synchronizované hodiny. Pomocí časového razítka lze zjistit i časové informace o zprávě.

6.2.3 Needham-Schroederův protokol

Je to autentizační protokol [13], použitelný ve dvou modifikacích:

- **Symetrický** – je založen na symetrické kryptografii. Tento typ je základem pro protokol Kerberos a využívá důvěryhodnou třetí stranu.
- **Asymetrický** – založen na vlastnostech asymetrické kryptografie. Není potřeba využívat důvěryhodnou třetí stranu. Komunikující strany mají k dispozici nástroj pro ověření pravosti veřejných klíčů.

Funkce symetrické modifikace je následující:

- Strana A odesílá důvěryhodné třetí straně (DTS) zprávu, která identifikuje stranu A i B a požaduje komunikaci se stranou B.
- DTS odpovídá šifrovanou zprávou pomocí sdíleného klíče , která obsahuje šifrovací klíč pro komunikaci a identifikaci protistrany. Dále obsahuje i šifrovanou zprávu pro stranu B. Ta opět obsahuje šifrovací klíč a identifikaci, tato zpráva je šifrována sdíleným klíčem strany B a DTS.
- Strana A dešifruje tuto zprávu, rozhodne o správnosti dat a vloženou šifrovanou část zprávy zašle straně B.
- Strana B dešifruje zprávu sdíleným klíčem s DTS a získá klíč pro komunikaci.
- Poté si obě strany pomocí náhodného čísla ověří, zda jsou schopny zprávu společným klíčem šifrovat a dešifrovat

6.2.4 Důvěryhodná třetí strana

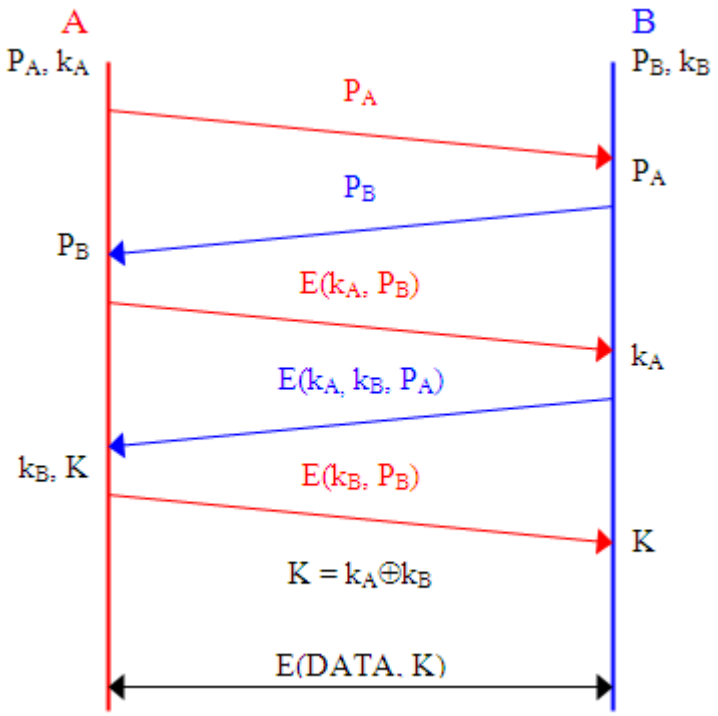
Pro určité typy autentizačních protokolů (Needham-Schroeder, Kerberos), je důležitým znakem důvěryhodná třetí strana [15]. Ve složitých sítích, kde spolu komunikuje více stran a které mají potřebu navazovat různé autentizované spojení, je výhodné jedné straně svěřit určité bezpečnostní funkce. Tato entita se nazývá důvěryhodná třetí strana a má funkci zprostředkovatele určitých bezpečnostních informací. Může sloužit jako úložiště pro tajné kryptografické klíče, databázi uživatelů a jiných informací. Pokud se vrátíme k Needham-Schroedrovu protokolu v symetrické podobě, vidíme, že obě strany využívají důvěryhodnou třetí stranu ke sdílení autentických veřejných klíčů protilehlých stran.

6.3 Řešení autentizace

Autentizace v sítích dálkového sběru dat by měla být oboustranná. Sběrová centrála by si měla autentizovat jednotlivé jednotky, protože případný útočník se může za jednotku vydávat a odesílat na centrálu nepravdivá data. Naopak jednotky by si měly chránit svůj obsah ve formě citlivých dat a autentizovat si protistranu, aby se případný útočník nemohl vydávat za sběrovou centrálu. Autentizaci není vhodné provádět za pomoci hesel, a to z důvodu velkého počtu jednotek a k tomu vztažené velké databázi hesel a jejich nesnadné aktualizaci. Vzhledem k velkému rozprostření jednotek a jejich vzdálenosti od sběrové centrály (dosah PLC až několik km) je nevhodné používat autentizace předmětem nebo žadatelem. Jako nejlepší možnost se jeví použití některých autentizačních protokolů či jejich modifikace spolu s šifrováním. Některé typy protokolů vyžadují důvěryhodnou třetí stranu, tato možnost je pro dálkový sběr dat až příliš složitá, a proto se jí dále nebudeme zabývat.

V systémech dálkového sběru dat po silových vedeních se jeví jako nejlepší způsob autentizace asymetrická kryptografie. V našem případě lze velice dobře aplikovat poměrně jednoduchý Needham-Schroedrův protokol v asymetrické modifikaci. To znamená, že obě strany znají systém symetrické a asymetrické šifry a mají k dispozici veřejné klíče asymetrické šifry protistrany. Tím si mohou vyměnit tajné klíče pro symetrickou šifru.

Komunikace by pak probíhala následovně:



Obr. 6: Návrh autentizace v sítích dálkového sběru dat

Při navazování spojení si strana A vygeneruje pár klíčů pro asymetrickou šifru a náhodné číslo k_A, poté odešle veřejný klíč straně B. Strana B si po přijmutí klíče vygeneruje klíče a náhodné číslo podobně jako protistrana a veřejný klíč opět poskytne protistraně. Pro tuto výměnu není potřeba zabezpečené komunikace, jakmile útočník bude chtít dešifrovat zašifrovanou zprávu tímto klíčem, vyjde mu nesmyslný shluk znaků.

Strana A přijme veřejný klíč P_B a pomocí tohoto klíče zašifruje asymetrickou šifrou náhodné číslo k_A. Vzniklý kryptogram $E(k_A, P_B)$ odešle protistraně. I když útočník zná veřejný klíč, který jsme zcela nepokrytě odeslali protistraně, není schopen tento kryptogram dešifrovat bez soukromého klíče, který zná pouze majitel veřejného klíče.

Strana B dešifruje tento kryptogram pomocí svého soukromého klíče a tím získá náhodné číslo klíč k_A. K tomuto číslu přidá své vlastní náhodné číslo k_B, zašifruje ho pomocí veřejného klíče P_A a tento kryptogram odešle protistraně.

Strana A kryptogram dešifruje svým soukromým klíčem a získá tím náhodné číslo k_B. Zároveň ověří, zda získané číslo k_A souhlasí s číslem, které poskytla protistraně.

Tím má strana A provedenou autentizaci, protože toto číslo mohla získat pouze osoba, která zná soukromý klíč asymetrické šifry. Strana A poté odešle kryptogram E (k_B, P_B).

Strana B si dešifrováním kryptogramu a úspěšným porovnáním získaného k_B s poskytnutým autentizuje protistranu. Tím je splněna oboustranná autentizace.

Obě strany pak po úspěšné autentizaci sečtou náhodná čísla k_A a k_B pomocí operace XOR (tab. 1) a tím vznikne klíč K, který je použit pro přenos dat pomocí symetrické šifry.

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

Tab.1 Operace XOR

Výsledkem průběhu komunikace je vzájemná autentizace a přenos klíče pro symetrickou šifru. Obě strany vědí, že klíč k_A (resp. k_B) vygenerovala pouze strana A (resp. B) a tím si jsou jisté identitou protistrany. Pravděpodobnost, že by se třetí strana C úspěšně vydávala za jednu z protistran a podařil se jí proces autentizace je velice malá. Výhodou tohoto typu autentizace je nízký počet šifrovacích operací a zasílaných zpráv.

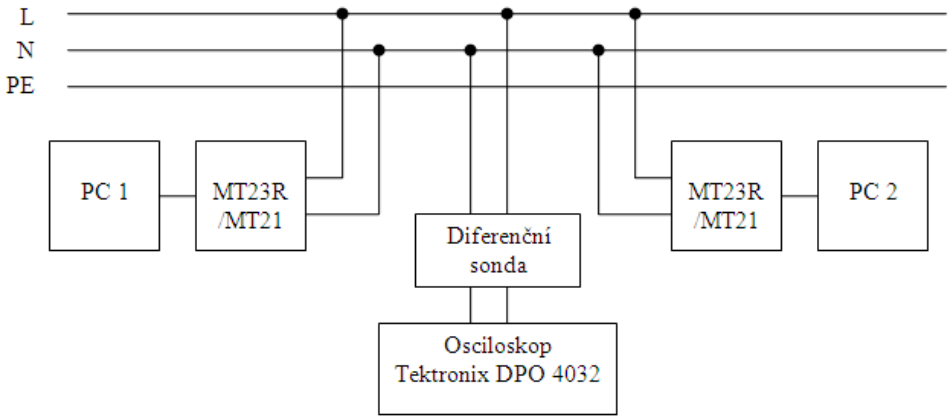
6.3.1 Obrana proti narušitelům

Na tento typ autentizace může být proveden útok zrcadlením, kdy útočník zpětně vysílá kryptogram stejné straně, která tento kryptogram odeslala. Obranou proti tomuto útoku je využití adres komunikujících stran v těle odesílaných zpráv. Protistrany jsou si pak jisté, že tento kryptogram odeslala protistrana a nejedná se o zrcadlení. Zároveň se jedná i o ochranu před odrazy ve vedení, na které jsou energetické sítě náchylné.

7 MĚŘENÍ SÍTĚ

7.1 Rušení

Pro měření rušení v laboratorních podmínkách jsme použili dvou počítačů s programem Hyperterminál, dvou sestav PLC modemu MT23R s napájecím a vazebním členem MT21 [9], dále pak osciloskop Tektronix DPO 4032 a diferenční sondu pro zobrazení průběhů na síti. Cílem měření bylo zobrazit možná rušení komunikace po rozvodné síti. Zapojení této soustavy je následné:



Obr. 7: Schéma zapojení při měření rušení

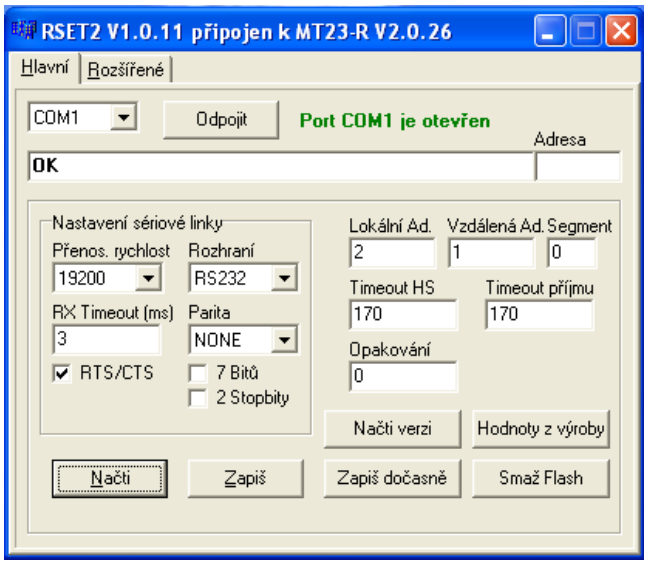
Modul MT21 [9]- slouží jako napájecí zdroj pro ostatní PLC moduly a zároveň splňuje funkci analogového vysílače a přijímače datových signálů do PLC sítě (energetické sítě 230V). S ostatními moduly je MT21 propojen pomocí plochého šestnáctižilového kabelu.

Modul MT23R [9]– je určen pro přenos dat po síti NN 230V 50Hz. Maximální délka datového bloku je 520 bajtů a je schopen komunikovat pomocí libovolného protokolu, který splňuje následující kritéria:

- je poloduplexní
- nekritický na dobu odezvy
- maximální délka zprávy je 520 bajtů

Efektivní rychlost přenosu dat se pohybuje okolo 5,5 kb/s a modul je schopný komunikovat až na vzdálenost 5km.

Nastavení modemu lze provádět pomocí programu RSET dodávaný výrobcem [9] a servisního kabelu RS232, který je zapojen do servisního portu modemu MT23R (jack 3,5mm) a RS232 portu počítače (canon 9). Nastavení sériové linky se týká pouze komunikačního portu modemu a pro účely našeho měření je zobrazeno na obr. 8.



Obr. 8: Nastavení modemů MT23R

Sériová linka je nastavena následovně:
- přenosová rychlost 19200 b/s
- rozhraní RS232
- parita žádná
- RX timeout 3 ms
- hardwarové řízení toku RTS/CTS.

Pro oboustrannou komunikaci musí být nastaveny adresy u obou modemů, jedná se o lokální a vzdálenou adresu. Adresy modemů jsou 1 a 2, lokální a vzdálená adresa se zvolí podle modemu, který je nastavován (na obr. 8 se jedná o modem s adresou 2).

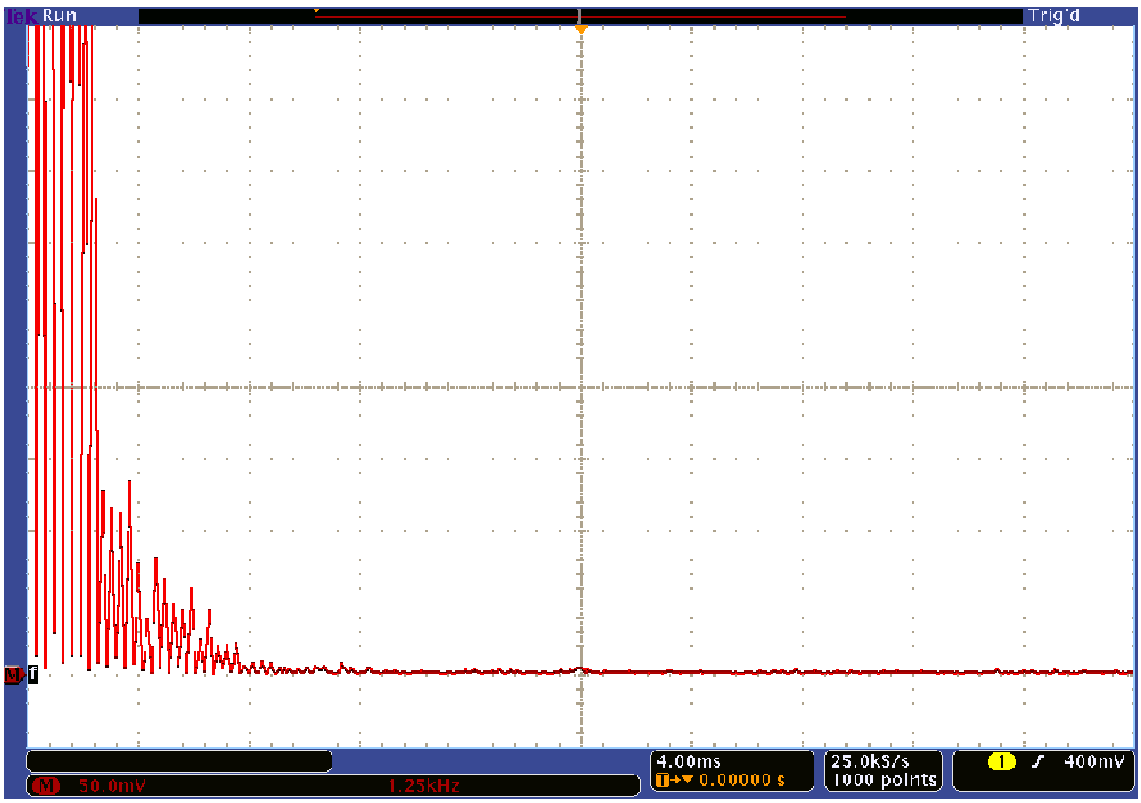
Diferenční sonda Metrix – pasivní diferenční napěťová sonda s dělícími poměry 1000:1, 100:1, 10:1

Tektronix DPO4032 – přenosný osciloskop vhodný pro servisní i laboratorní použití. Šířka pásma 350 MHz, 2 kanály s rychlostí vzorkování až 5 GS/s a pamětí 10 MS.

Modem MT23R je úzkopásmový modem komunikující v pásmu stanoveným evropskou normou EN 50065–1 [14]. Rozsah tohoto pásma je 9-148,5kHz, proto jsme pomocí

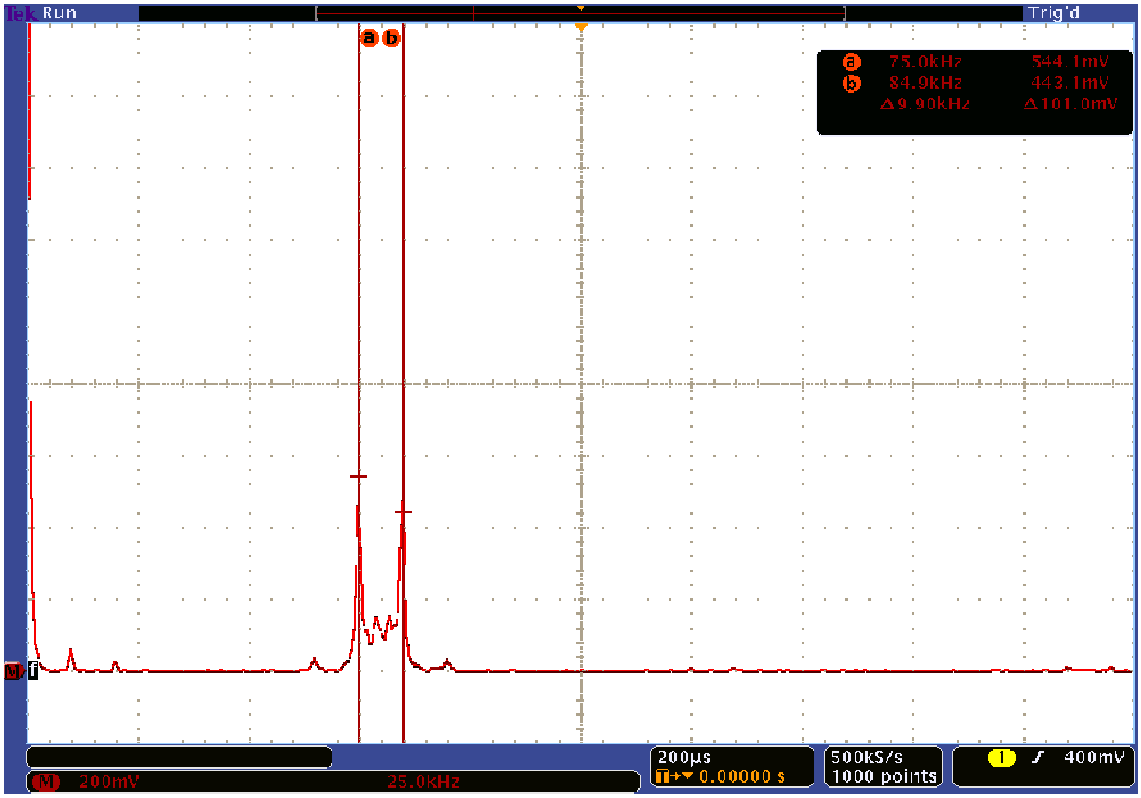
osciloskopu sledovali rušení přibližně v tomto pásmu. Zobrazení probíhalo pomocí matematické funkce FFT a hammingova okna.

Nejprve jsme provedli měření sítě bez jakéhokoliv rušení a komunikace mezi modemy. Z výsledného spektra je patrné, že přibližně do 1,25kHz je amplituda šumu větší než 100mV. Avšak komunikační pásmo modemů podle normy EN 50065-1 [14] začíná až na frekvenci více něž sedminásobné. Proto se nepředpokládá jakékoliv rušení komunikace mezi modemy. Tento šum vzniká nelineárními spotřebiči připojenými do sítě. Zbytek spektra se zdá být poměrně čistý a bez jakéhokoliv většího rušení ovlivňujícího komunikaci.



Obr. 9: Spektrum energetické sítě

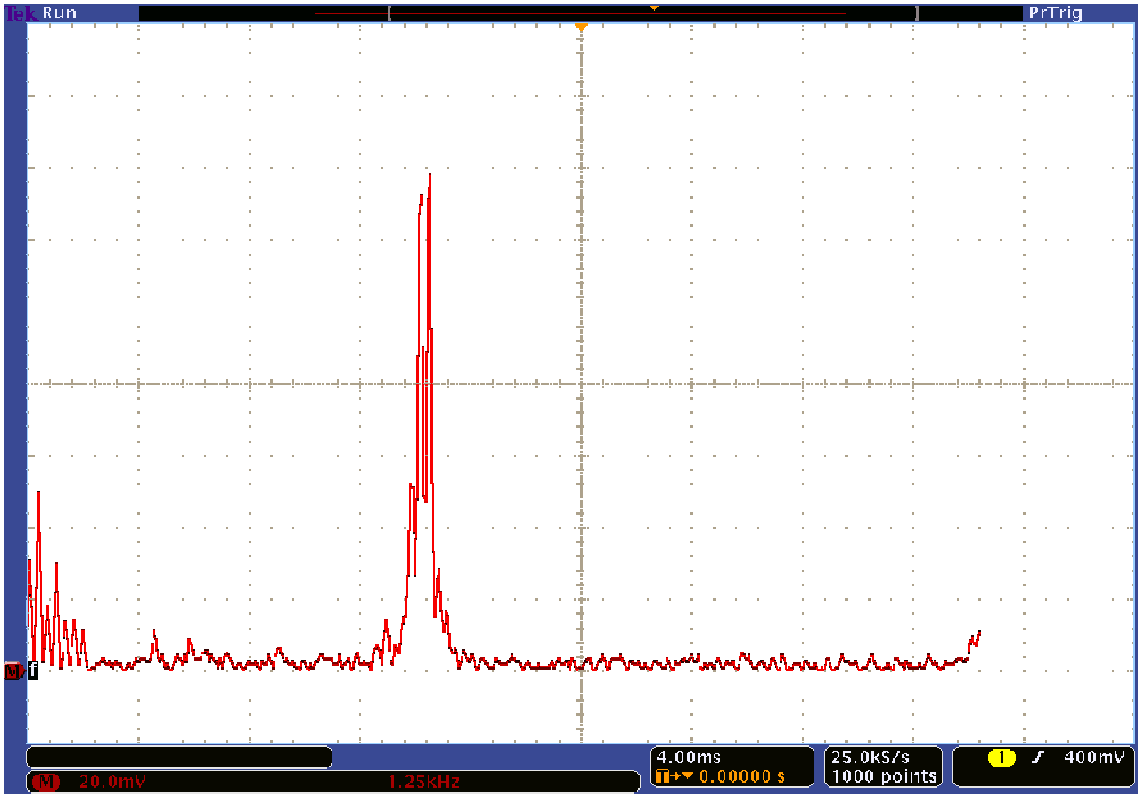
V další části měření jsme pomocí programu Hyperterminál přenášeli soubor mezi oběma PC. Spektrum na obr. 10 zobrazuje vlastní komunikaci mezi modemy, která probíhá kolem 80kHz. Toto pásmo má šířku přibližně 10kHz a obsahuje dvě špičky na 75kHz a 85kHz a jejich amplituda se pohybuje kolem 500mV. Případné rušení této komunikace by muselo mít přibližně tuto amplitudu.



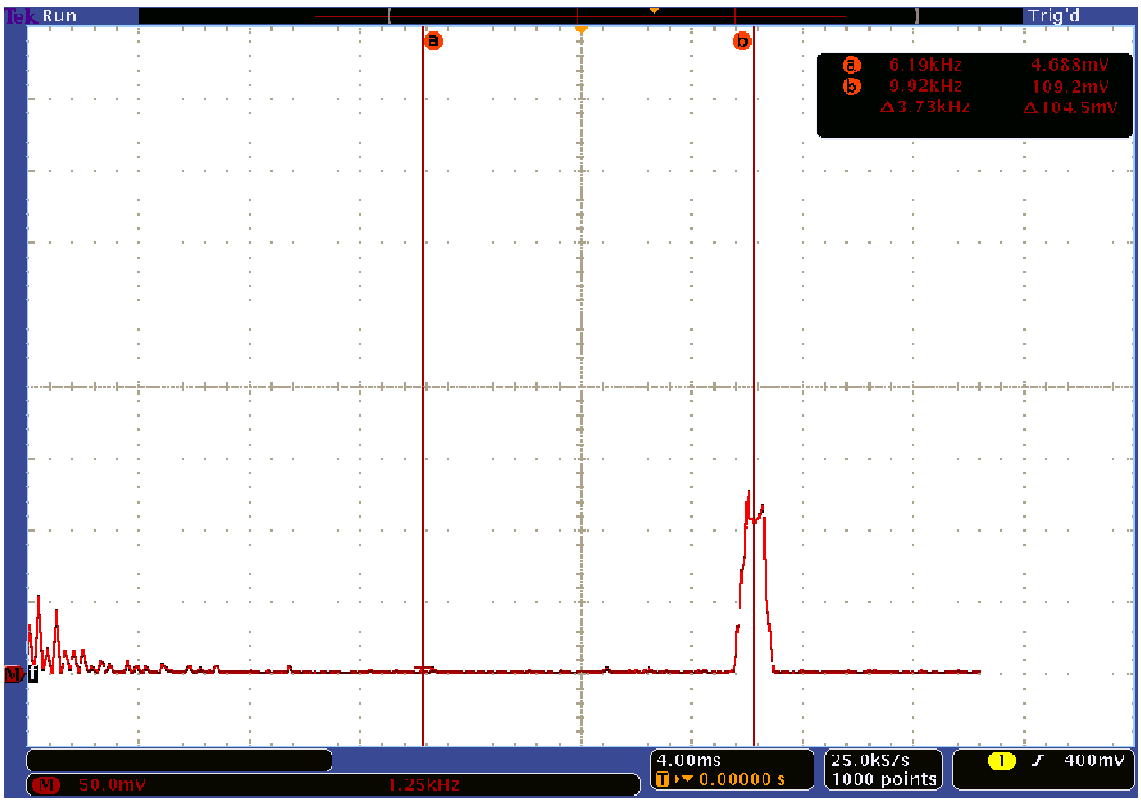
Obr. 10: Spektrum komunikace modemů MT23R

Následně probíhaly pokusy o rušení této komunikace asynchronním motorem s výkonem 720W. Spektrum je zobrazeno na obr. 11. Je zde patrné rušení od tohoto motoru okolo frekvence 6kHz s nezanedbatelnou amplitudou 120mV. Opět je ale toto rušení mimo normované pásmo a dokonce i mimo pásmo komunikace modemů, proto se rušení asynchronním motorem neprojeví na komunikaci.

Vyzkoušeli jsme několik typů přístrojů s asynchronním motorem, avšak toto rušení bylo největší, kterého jsme dosáhli. Rušení se v jednom případě dokonce objevovalo na více frekvencích, ale nemělo dostatečnou amplitudu.



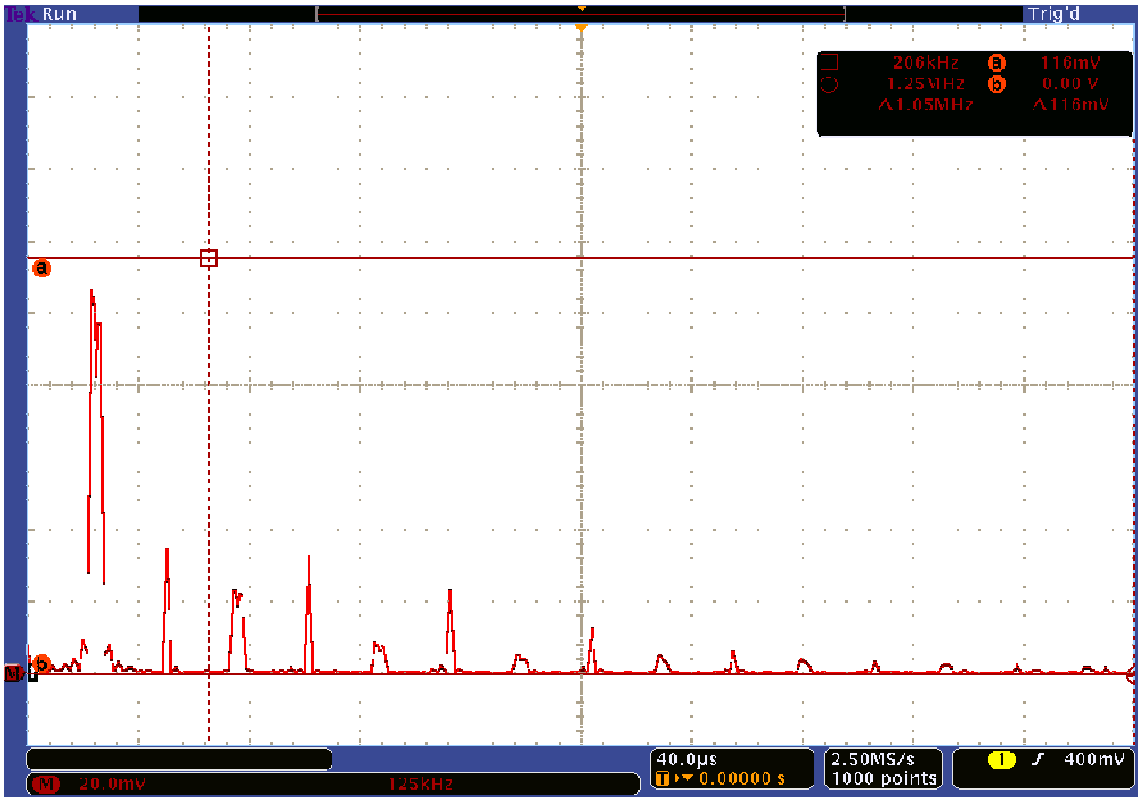
Obr. 11: Rušení asynchronním motorem



Obr. 12: Rušení vzniklé od spínaného zdroje PC

Rušení vzniklé spínaným zdrojem PC o výkonu 400W se projevovalo jako úzké pásmo kolem 10kHz s amplitudou přibližně 110mV (obr. 12). Ani tento spínaný zdroj není schopen narušit komunikaci modemů, avšak některé spínané zdroje nebo záložní zdroje UPS vykazují velmi nízkou impedanci vůči přenosovým signálům a mohou způsobit přerušení komunikace. Takový spínaný zdroj se nám nepodařilo objevit.

V praxi je tedy velice nesnadné najít přístroj, který by rušil úzkopásmovou komunikaci modemů MT23R a případné rušení těchto modemů má náhodný charakter u jednotlivců.

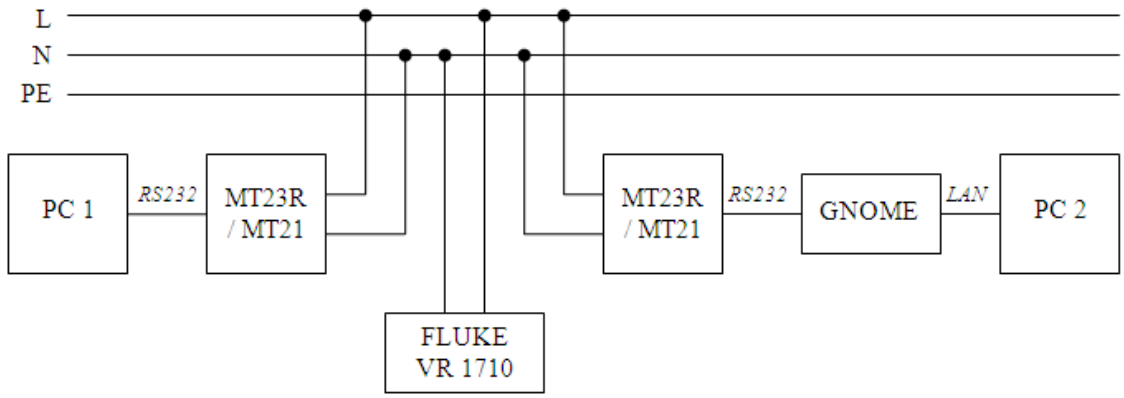


Obr. 13: Harmonické modemů MT23R

Paradoxní je, že i sám přenos způsobuje rušení v podobě harmonických (obr. 13). Je vidět, že až 5. harmonická má alespoň 35% amplitudu v poměru k hlavní. Což může způsobovat rušení jiných přístrojů připojených k rozvodné síti.

7.2 Testování sítě

Dlouhodobé testování sítě spočívalo na sledování vlivu kvality elektrické energie na přenosovou rychlost modemů a naopak, tedy vlivu PLC komunikace na kvalitu elektrické energie po dobu 24 hodin. Oproti předchozímu zapojení jsme navíc použili záznamník kvality elektrické energie FLUKE VR 1710 [12] a převodník GNOME232 [10] pro prodloužení sériové linky po síti LAN. Délka elektrického vedení je přibližně 50 metrů. Pro měření jsme použili schéma zapojení na obr. 14.



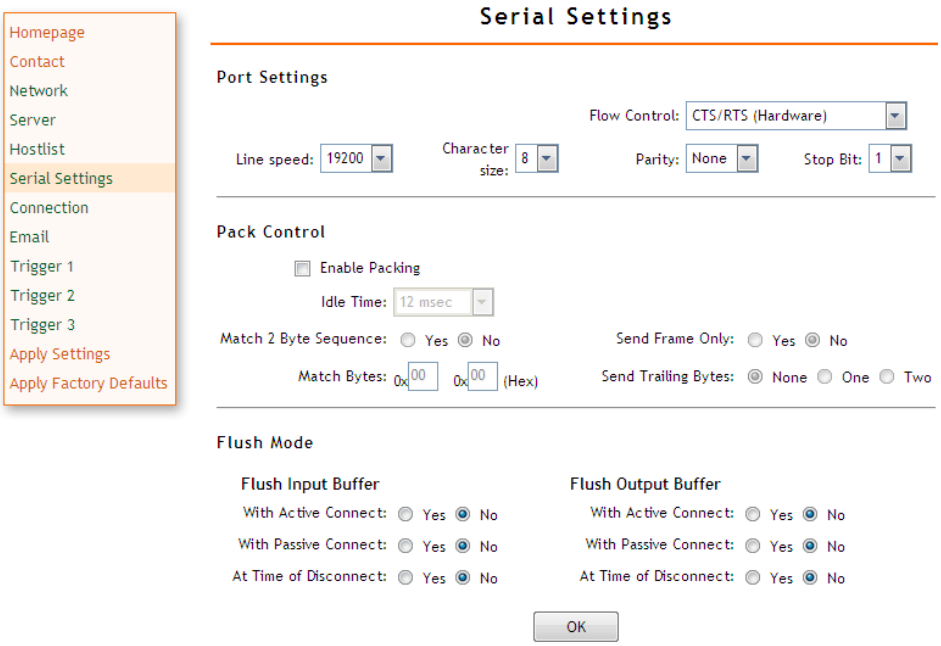
Obr. 14: Schéma zapojení při testování stě

FLUKE VR 1710 [12]– je jednofázový, zásuvný záznamník kvality napětí, který zjišťuje a zaznamenává problémy s kvalitou elektrické energie. Parametry elektrické energie zahrnují hodnotu RMS, přechodové jevy, flikr (mihotání světel) a harmonické kmity až do 32. jsou zaznamenávány pomocí uživatelem definované průměrné doby od 1 sekundy do 20 minut.

V našem případě jsme použili dobu měření 2 sekundy. Ke zpracování dat byl použit program Power Log, dodávaný spolu se zařízením.

GNOME232 [10]– jednoduchý převodník rozhraní Ethernet na sériovou linku RS232. Tento převodník umožňuje jednoduché připojení přístrojů s rozhraním RS232 na Ethernet nebo prodloužení sériové linky přes Internet kamkoliv na světě. Součástí je “virtuální sériový port“ [10], tedy software, který v operačním systému Windows vytvoří nový sériový port přesměrovaný přes Ethernet na modul GNOME232. Lze tedy použít programy, které komunikují přes sériový port a nejsou navrženy pro komunikaci přes Ethernet.

Převodník GNOME 232 byl zapojen do sítě LAN a pro jeho konfiguraci bylo použito webové rozhraní. Po nastavení přístupové adresy, portu a parametrů sériové linky jsme přistoupili ke spuštění virtuálního sériového portu na portu COM20. Poté jsme spustili na obou počítačích program Hyperterminál a spustili jsme komunikaci.

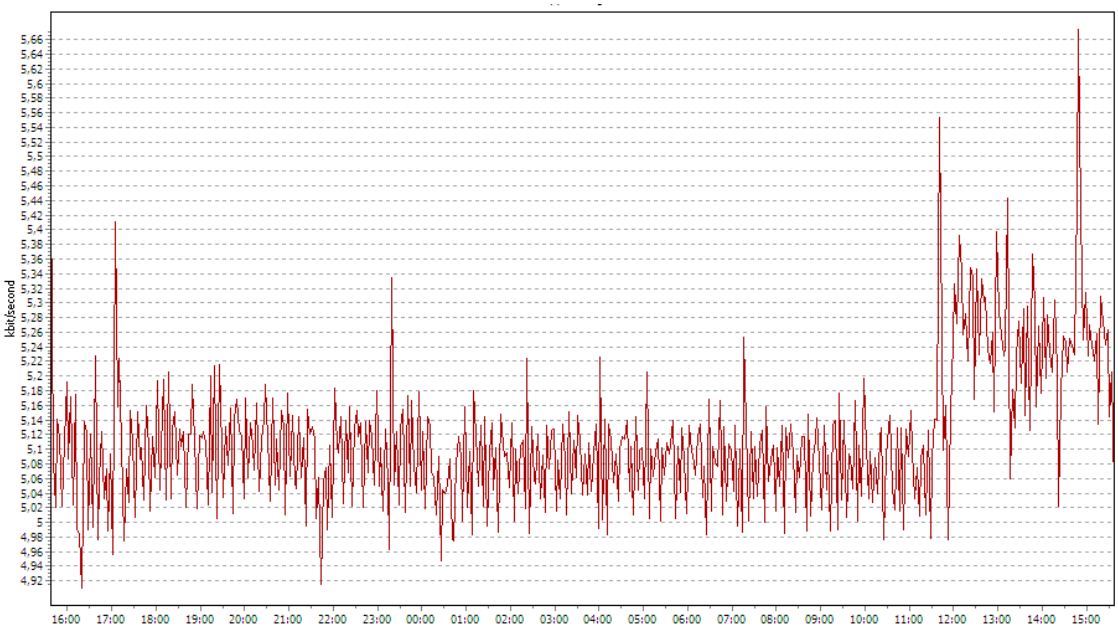


Obr. 15: Nastavení sériového portu pomocí webového rozhraní

7.2.1 Měření rychlosti komunikace

Měření rychlosti komunikace jsme prováděli dlouhodobě a to po dobu 24 hodin. Během této doby jsme pomocí programu Hyperterminál přenášeli soubor a zároveň byla zaznamenávaná data o kvalitě sítě během tohoto přenosu. K zaznamenávání dat byl použit analyzátor FLUKE [12].

Rychlost přenosu byla zaznamenávána pomocí programu PRTG Traffic Grapher [16]. Program pracuje na principu internetového protokolu SNMP (Simple Network Managment Protocol), který podporuje převodník GNOME232. Umožňuje průběžný sběr dat pro potřeby správy sítě, a jejich následné vyhodnocování. Data k výpočtu rychlosti byla aktualizována každých 30 vteřin a graf byl sestaven z tříminutových průměrů.



Obr. 17: Rychlost komunikace

Průměrná rychlost přenosu byla 5,1 kbit/s. Tato rychlost neodpovídá přímo přenosové rychlosti po energetické síti, avšak má s touto rychlostí přímou spojitost a dá se považovat za použitelnou k analýze přenosu.

Rychlost komunikace je do 12. hodiny přibližně stejná, náhlé zvýšení přenosové rychlosti o 0,15 kbit/s se dá považovat za náhodné, protože analýzou získaných dat o kvalitě elektrické energie nebyla nalezena žádná interakce mezi rychlostí komunikace a jednotlivými parametry těchto dat. Zároveň je toto zvýšení zanedbatelně malé.

Měření tedy neprokázalo nějakou spojitost parametrů kvality elektrické energie zaznamenané analyzátorem FLUKE s přenosovou rychlostí modemů.

7.2.2 Vliv komunikace na kvalitu elektrické energie

V dalším měření jsme hodnotili vliv komunikace po síti na kvalitu elektrické energie dodávané touto sítí. Opět bylo použito zapojení podle obr. 14. Nejdříve byly po dobu 24 hodin zaznamenávané parametry sítě bez probíhající komunikace mezi modemy a poté dalších 24 hodin se spuštěnými modemy a přenosem dat. Přenos dat probíhal pomocí programu Hyperterminál po celou dobu druhého čtyřiadvaceti hodinového měření. K záznamu parametrů elektrické energie byl použit záznamník FLUKE, který zaznamenává tyto hodnoty:

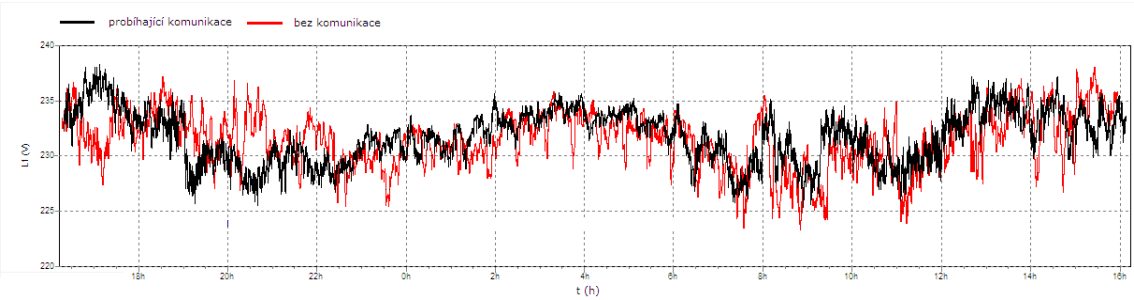
RMS hodnota střídavého napětí – je to efektivní hodnota střídavého napětí a je rovna hodnotě stejnosměrného napětí, které by po přiložení na odporovou zátěž dávalo stejný průměrný výkon. V praxi se v silnoproudé elektrotechnice téměř vždy předpokládá, že jde o efektivní hodnoty.

Síťová frekvence – jmenovitý kmitočet napájecího napětí. V české republice se v distribučních sítích používá jmenovitá frekvence 50Hz.

Flikr – elektrické spotřebiče (např. žárovky) připojené do veřejné distribuční sítě, vyžadují pro správnou funkci konstantní napětí. Odběratelé s proměnlivým výkonem však bohužel způsobují měnící se úbytky napětí. Tyto rychlé periodické změny napětí nazýváme flikr. Projevuje se změnou zrakového vnímání, která ruší člověka při jeho činnosti. Tyto změny jsou vyvolány časovými změnami světelného toku vlivem rychlých změn napětí.

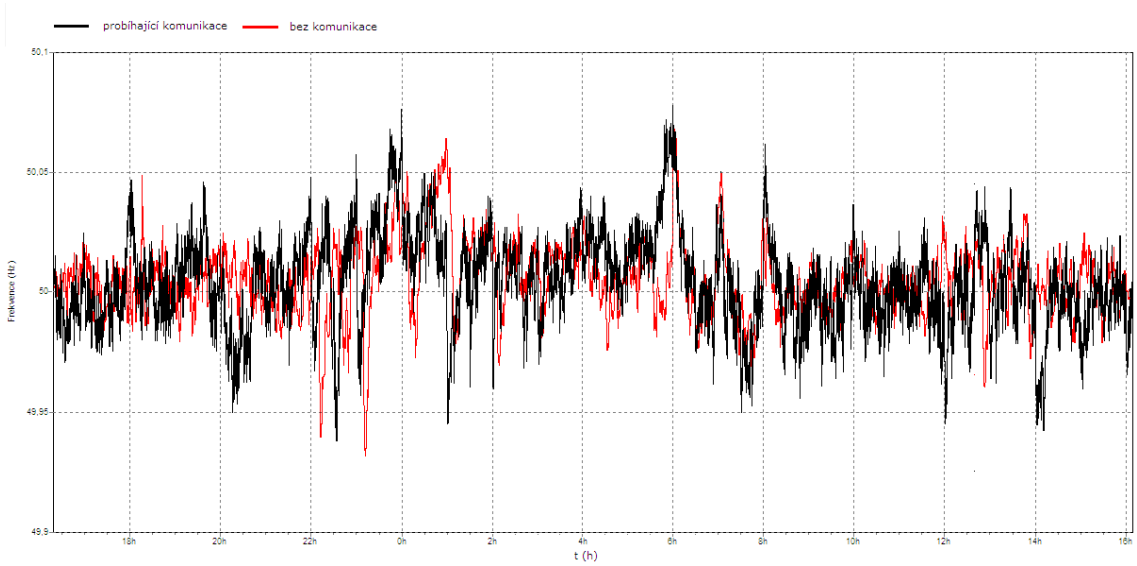
Harmonické složky – složky, které mají frekvenci větší než 50Hz (základní harmonická), se nazývají harmonické. Harmonické proudy tečou od nelineárních spotřebičů do sítě a vyvolávají úbytky na impedanci sítě. Tyto úbytky vedou k deformacím časového průběhu napětí. Harmonické charakterizujeme jejich frekvencí (např. 200Hz) nebo jejich poměrem k základní harmonické(např. 200/50 = 4).

Prvním parametrem, který je analyzován záznamníkem FLUKE, je RMS hodnota síťového napětí. Na obr. 18 jsou průběhy tohoto napětí měřené bez a s přenosem dat. Po většinu času je síťové napětí v obou měřeních přibližně stejné. Případné výkyvy mezi 16. a 22. hodinou jsou způsobeny děním v síti a nemají spojitost s PLC komunikací, protože po zbytek dne je síťové napětí identické pro obě měření. Proto lze usoudit, že PLC modemy a jejich komunikace nemají na RMS hodnotu síťového napětí žádný vliv.



Obr. 18: Průběh napětí

Dalším parametrem kvality elektrické energie je síťová frekvence. Průběhy frekvence bez komunikace a s probíhající komunikací v časovém období 24 hodin jsou zobrazeny na obr. 19. Oba průběhy jsou téměř identické. Měření tedy neprokázalo vliv komunikace po vedení elektrické energie na frekvenci síťového napětí.

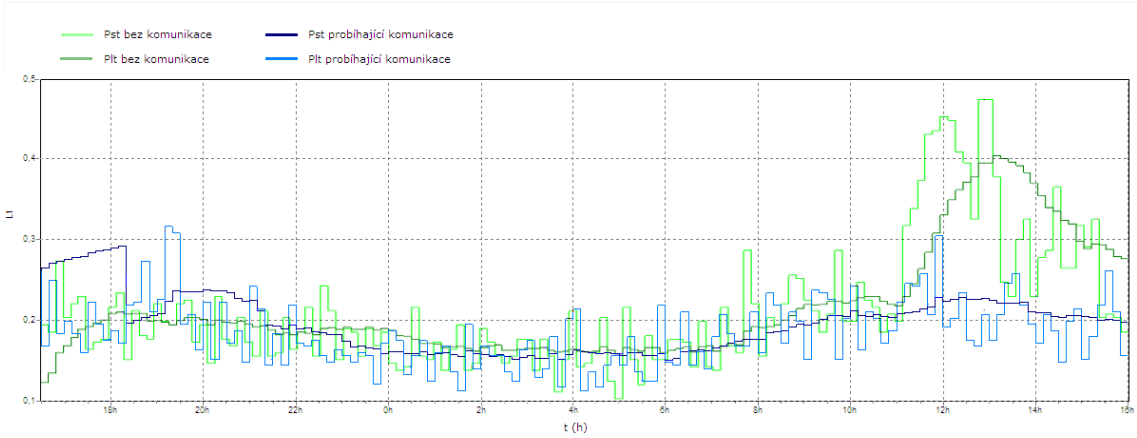


Obr. 19: Síťová frekvence

Záznamník kvality elektrické energie zaznamenává i jev zvaný flikr. Je způsoben rychlými periodickými změnami napětí a projevuje se změnou zrakového vnímání, která ruší člověka při jeho činnosti. Tyto změny jsou vyvolány časovými změnami světelného toku vlivem rychlých změn napětí. Záznamník měří dva parametry tohoto jevu:

P_{st} – krátkodobá míra vjemu blikání

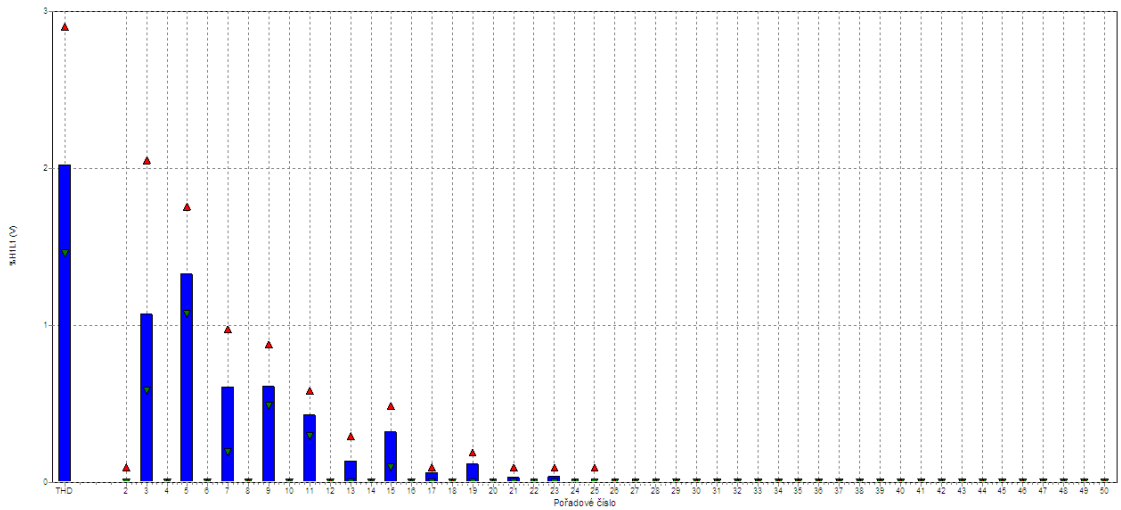
P_{lt} - dlouhodobá míra vjemu blikání



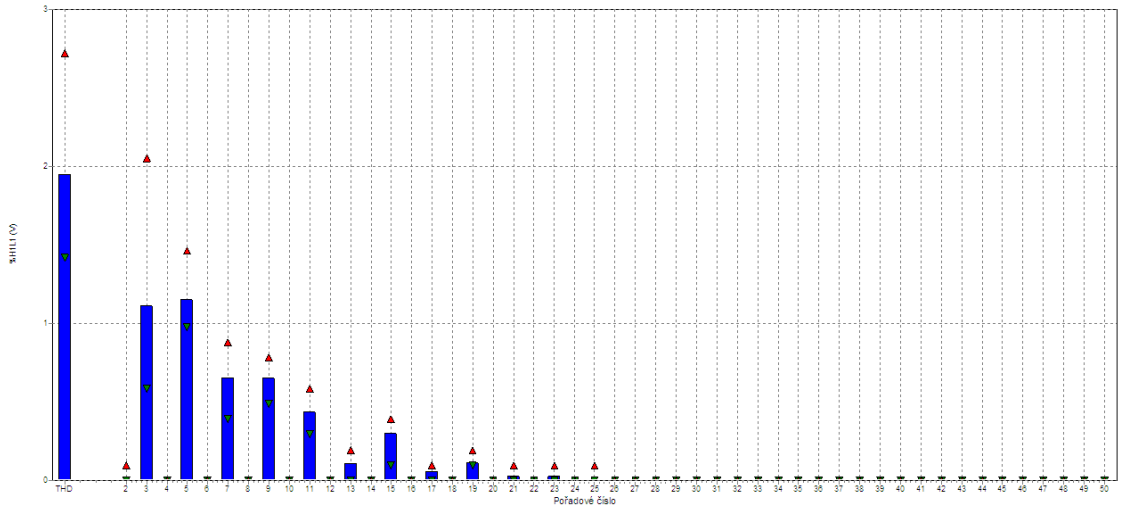
Obr. 20: Flikr

Na obr. 20 je patrné, že flikr je po většinu času měření přibližně stejný. Výkyvy po 12. hodině jsou způsobeny děním v síti a s komunikací PLC modemů nemají nic společného. V nočních hodinách je vidět průběh flikru při obou měřeních a tyto hodnoty jsou identické, proto se dá konstatovat, že vliv komunikace na tento parametr kvality elektrické energie je nulový.

Záznamník kvality FLUKE dále měří jednotlivé složky, které mají frekvenci větší než 50Hz (základní harmonická), nazývají se harmonické. Harmonické proudy tečou od nelineárního spotřebiče do sítě a vyvolávají úbytky na impedanci sítě. Tyto úbytky vedou k deformaci časového průběhu napětí v porovnání s relativně čistým sinusovým průběhem. Harmonické charakterizujeme jejich frekvencí nebo poměrem jejich frekvence k frekvenci základní harmonické (např. 250/50 = 5).



Obr. 21: Harmonická napětí bez komunikace



Obr. 22: Harmonická napětí při komunikaci

I z těchto grafů je patrné, že žádná změna v průběhu komunikace nenastala. Proto PLC komunikace po elektrické síti nemá vliv na vznik harmonických k základní harmonické 50Hz.

Závěrem tohoto měření se dá prohlásit, že vliv PLC komunikace modemů MT23R nemá žádný vliv na kvalitu elektrické energie dodávané sítí, po které tato komunikace probíhá. Všechny parametry měřené záznamníkem kvality FLUKE zůstaly v nezměněné podobě bez komunikace a při komunikaci po síti. Proto se není třeba obávat jakýchkoliv změn kvality elektrické energie při používání těchto modemů.

7.3 Analýza paketů

K analýze paketů jsme použili schéma zapojení na obr. 14 a pokusili jsme se zachytávat komunikaci na síti LAN mezi převodníkem GNOME232 [10] a PC2. K tomu jsme využili pro zachytávání paketů program Wireshark[18] a ke komunikaci program Docklight [17]. Výsledkem tohoto měření má být zjištění, v jaké formě jsou posílána data pomocí PLC modemů.

Pomocí programu Docklight jsme si postupně z obou PC odeslali sekvenci dat, kterou jsme zachytávali programem Wireshark a poté jsme tyto pakety analyzovali.

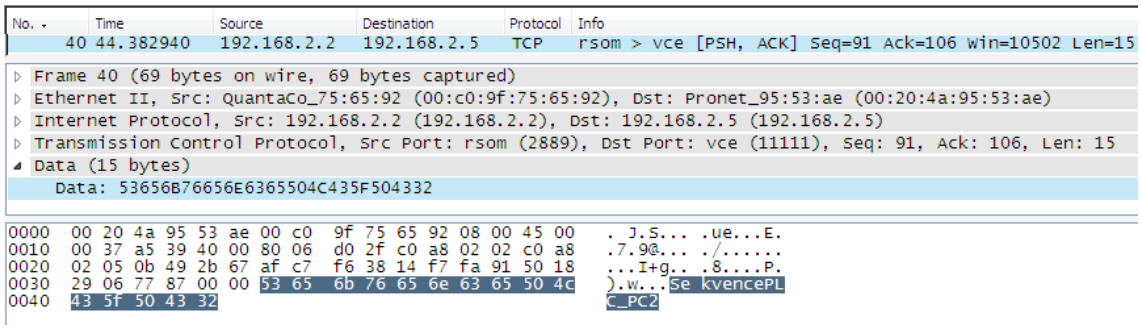
Sekvence měli takovouto podobu:

od PC1 k PC2 – SekvencePLC_PC1 (15B)

od PC2 k PC1 – SekvencePLC_PC2 (15B)

Ethernetový rámec je podle směru přenosu vytvořen buď programem pro vytvoření virtuálního sériového portu [10] (směr PC2 **à** PC1), nebo převodníkem GNOME232 [10] (směr PC1 **à** PC2).

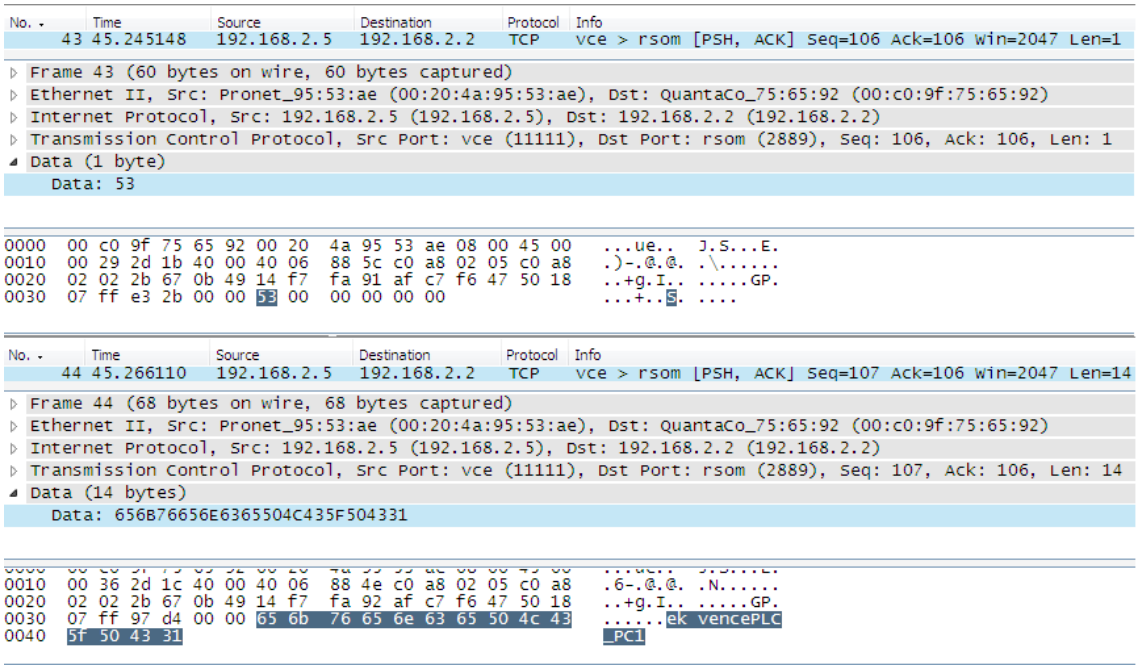
Na paketu (obr. 23) zachyceném programem Wireshark je vidět komunikace PC2 s PC1. V tomto rámci jsou data vložená „virtuálním sériovým portem“ a představují data posílaná programem Docklight po sériové lince.



*Obr. 23: Zachycený paket PC2 **à** PC1*

Je vidět, že velikost dat i obsah zůstal v nezměněné podobě. Z toho vyplývá, že ani jeden z použitých programů nijak odesílaná data nemění. Teď už víme, že program Docklight odesílá pouze zadaná data bez přídavných informací.

To je důležité, hlavně pro opačný směr, kdy tato data jsou nejdříve přenášena pomocí modemů a teprve pak je vytvořen ethernetový rámec převodníkem GNOME232 [10]. Tato komunikace je vidět na obr. 24. Odesílaná data jsou sice rozdělena do dvou rámců, ale odesílaná sekvence má stejnou velikost a zůstala v nezměněné podobě. Lze tedy říct, že použité modemy MT23R [9] posílají data po sériové lince bez přídavných informací.



*Obr. 24: Zachycené pakety PC1 **à** PC2*

8 ZÁVĚR

V této práci jsme si nejprve přiblížili PLC přenos z hlediska technologie a využití. Poté jsme popsali vlastnosti silových vedení a rušení vyskytující se na tomto vedení. Tato vedení se zdají pro komunikační technologie velice nepřátelská a nejsou pro tento účel primárně navrženy. Navíc se na těchto vedeních vyskytuje mnoho typů rušení a šumu, který také výrazně ovlivňuje kvalitu komunikace. Některé z těchto problémů se dají úspěšně minimalizovat výběrem vhodné modulace a vhodného protichybového kódování. Pro účely PLC se jeví jako nejvhodnější modulace OFDM, avšak záleží na způsobu použití.

Pro autentizaci v systémech dálkového sběru dat se zdá být nejvhodnější asymetrická kryptografie, která poskytuje jednodušší distribuci klíčů. Pro tyto systémy jsme navrhnuli schéma autentizace založené na Needham-Schroedrovu protokolu.

V další části probíhalo měření s modemy MT23R firmy Modemtec. Zobrazili jsme si základní typy rušení a spektrum komunikace modemů. Ze spektra je viditelné, že modemy komunikují na frekvencích okolo 80 kHz a šířka pásma je okolo 10 kHz. Dokázali jsme, že komunikaci mezi modemy je velice nesnadné přerušit. Rušení by muselo probíhat přímo na frekvencích, na kterých modemy komunikují.

Měřením bylo také zjištěno, že tyto modemy nemají vliv na základní parametry energetické sítě a přenosová rychlost zůstává se změnou těchto parametrů konstantní. Proto lze modemy používat i v prostředích náchylnějších na změny primárních parametrů.

Zachytáváním paketů jsme stanovili, že modemy při komunikaci nepřidávají žádná přebytečná data a po sériové lince posílají pouze čistá data odeslaná jednotlivými programy.

9 POUŽITÁ LITERATURA

[1] Hrasnica, Haidine, Lehnert, Broadband Powerline Communications Network Design, ISBN: 0-470-85741-2, 2004.

[2] Pužmanová, R., Data po elektrické síti [online], Dostupné z: http://www.etm.cz/obr/datapoelsiti.pdf, 2004.

[3] M. Zimmermann, K. Dostert, The low voltage distribution network as last mile access network - signal propagation and noise scenario in the HF- range, AEU International Journal of Electronics and Communications, 2000, č. 1, s. 13 – 22

[4] Trnka, M., Komunikace po napájecí (rozvodné) síti. Slaboproudý rozvod, 2005, č. 2, s. 14 - 18

[5] Filka, M., Přenosová média. Skriptum VUT FEKT.Brno, VUT FEKT, 2002

[6] Němec, K., Datová komunikace. Skriptum VUT FEKT Brno, VUT FEKT, 2007

[7] Pavelka, O., Internet ze zásuvky? Ano, ale… [online]. Dostupné z: http://www.elektrorevue.cz/clanky/00034/index.html, 2000

[8] Burda, K., Bezpečnost informačních systémů. Skriptum VUT FEKT Brno, VUT FEKT, 2005

[9] ModemTec. www.modemtec.cz [online]. 2006, [cit. 28.4.2009]. Dostupné z URL: <http://www.modemtec.cz/moduly.php>

[10] Papouch s.r.o. GNOME232 - převodník Ethernet RS232 [online]. 2009, [cit. 28.4.2009]. Dostupné z URL: < http://www.papouch.com/shop/scripts/ _detail.asp?katcislo=0285>

[11] Menezes A. J. Handbook of applied cryptography. CRC Press, 1996. Dostupné z URL: <http://www.cacr.math.uwaterloo.ca/hac/> ISBN 0-8493-8523-7

[12] FLUKE. Záznamník kvality napětí Fluke VR1710 [online]. 2009, [cit. 5.5.2009]. Dostupné z URL: < http://fluke.cz/comx/show_product.aspx?locale= czcs&pid=37819>

[13] DIMACS, Needham-Schroeder Public Key Protocol [online]. 2009, [cit. 14.4.2009]. Dostupné z URL: < http://dimacs.rutgers.edu/Workshops/Security/ program2/boyd/node14.html>

[14] ČSN EN 50065-1 - Signalizace v instalacích nízkého napětí v kmitočtovém rozsahu 3 kHz až 148,5 kHz - Část 1: Všeobecné požadavky, kmitočtová pásma a elektromagnetická rušení. Praha: Český normalizační institut, 2002.

[15] Staudek J., Hanáček P. Bezpečnost informačních systémů. ÚSIS Praha, 2000. Dostupné z URL: < http://www.cs.vsb.cz/ochodkova/courses/kpb/usis_prirucka_brezen.pdf>

[16] PAESSLER. PRTG traffic grapher. 2009 [online]. Dostupné z URL: <http://www.paessler.com/prtg6>

[17] Flachmann M., Heggelbacher O. Docklight [Online]. 2009. .Dostupné z URL: <http://www.docklight.de>

[18] Combs G. Wireshark. 2009 [Online]. Dostupné z URL: <http://www.wireshark.org/download.html>